LDI NRW

30. Bericht

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen



30. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Bettina Gayk

zum Datenschutz
für die Zeit vom 1. Januar 2024
bis zum 31. Dezember 2024

und zur Informationsfreiheit
für die Zeit vom 1. Januar 2023
bis zum 31. Dezember 2024

Inhalt

1. Teil: Datenschutzbericht **9**

1. Vorwort **9**

2. Datenschutz in Europa **13**

3. Datenschutz in Deutschland **17**

4. Änderung des Bundesdatenschutzgesetzes darf nicht auf die lange Bank geschoben werden **21**

5. Künstliche Intelligenz **25**

5.1. Künstliche Intelligenz und der Datenschutz: Was Verantwortliche beachten sollten 25

5.2. Die neue EU-Verordnung über künstliche Intelligenz: Einige Probleme müssen noch gelöst werden 27

5.3. Generative Künstliche Intelligenz: Was gilt für die Betroffenenrechte? 31

5.4. Emotionserkennungssoftware hat im Callcenter nichts zu suchen 36

6. Internet, Medien und Digitales **41**

6.1. Gibt es ein Recht auf ein analoges Leben? 41

6.2. Datenschützer*innen stellen strengere Regeln für Website-Betreiber*innen auf 43

7. Schule und Bildung **47**

7.1. Gute Nachricht bei der Digitalisierung der Schule – Forschungsprojekt DIRECTIONS kommt voran 47

7.2. iPads im Unterricht: Landesdatenschutzbeauftragte gibt Hinweise zur datenschutzgerechten Nutzung 48

7.3. Wenn LeOn in der Schule mithört – Tonaufzeichnungen verlangen eine Einwilligung 53

8. Verwaltung, Inneres und Justiz **55**

8.1. Geplantes Sicherheitspaket der Landesregierung – Bitte keine Schnellschüsse! 55

8.2. Kontrollbefugnis der LDI NRW über die Staatsanwaltschaften – Konflikt besteht weiterhin 58

8.3. LDI NRW behält Datenverarbeitung bei der Polizei im Blick 61

8.4. Polizeibehörden – Finger weg von der WhatsApp-Nutzung! 64

8.5. Verkehrsunfall: Polizei darf Zeugendaten nicht einfach weitergeben 66

8.6. Daten von Zeug*innen sind sensibel – auch wenn es nur um Ordnungswidrigkeiten geht 68

8.7. Fotos von Falschparker*innen aufnehmen? In der Regel ist das ok 71

8.8. Helfer*innen auf Großveranstaltungen dürfen nicht einfach reihenweise von der Polizei durchleuchtet werden 73

8.9. Corona-Hilfen: Fluten mit Auskunftsanträgen macht einzelnen Antrag nicht automatisch rechtsmissbräuchlich 75

9. Gesundheit und Soziales 79

9.1. Die Pandemie ist vorbei, die Missachtung des Datenschutzes geht weiter 79

9.2. Bezahlkarte für Geflüchtete: Diese wichtigen Punkte müssen bei der Einführung beachtet werden 82

9.3. Auskunft vom Jugendamt? Eltern haben hier nur eingeschränkte Rechte 84

9.4. Telefonnummer und E-Mail-Adresse müssen beim Jobcenter nicht angegeben werden 86

10. Wirtschaft 89

10.1. Neue Leitlinien: Europäische Aufsichtsbehörden erläutern wichtige Rechtsgrundlage für Datenverarbeitung durch Unternehmen 89

10.2. Betrugsbekämpfung in der EU: LDI NRW setzt sich für klare Regeln beim Austausch von Zahlungsdaten ein 92

10.3. Unternehmensverkauf per Asset Deal: Neue Orientierungshilfe klärt wichtige Fragen zum Datenschutz 95

10.4. Wirtschaftsauskunfteien erhalten neue Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten 98

10.5. LDI NRW bringt Datenschutz-Zertifizierung in Deutschland weiter voran – Angebot wird erweitert 100

10.6. Wirtschaftsauskunfteien: Beim Scoring muss weiter kontrolliert werden 102

10.7. Betrugsprävention ja – aber bitte datenschutzkonform! LDI NRW geht gegen Austausch von Gesundheitsdaten vor 105

11. Werbung 107

11.1. Pur-Abo-Modelle machen Schule – Datenschutzbehörden stellen Regeln auf 107

11.2. Welche Verhaltensregeln gelten beim grenzüberschreitenden Direktmarketing per Post? 110

11.3. Wenn Banken die Zahlungsverkehrsdaten zu Werbezwecken nutzen 113

11.4. Dreiste Werbung – LDI NRW leitet Bußgeldverfahren gegen Telekommunikationsunternehmen aus NRW ein 115

12. Wohnen **119**

12.1. Wärmebilder von Häusern können beim Energieeinsparen helfen – wenn die Rechte der Nachbar*innen beachtet werden 119

12.2. Smart Metering: Neue Orientierungshilfe hilft im Umgang mit funkbasierten Strom-, Heizungs- und Wasserzählern 123

12.3. Stadtwerke sollten WhatsApp nicht beim Zählerablesen einsetzen 125

12.4. Rauchmelder mit Klima-Monitoring müssen erst einmal ausgeschaltet sein 127

12.5. Smarte Geräte im Haushalt – Käufer*innen wie Hersteller*innen sollten Sorgfalt walten lassen 130

13. Videoüberwachung **135**

13.1. Videoüberwachung im Außenbereich eines Museums? Ohne konkrete Gefährdung gibt es enge Grenzen 135

13.2. Keine ungeschwärzte Akteneinsicht, um Informant*innen zu enttarnen – Gericht stützt Haltung der LDI NRW 139

14. Datenschutz im Verein **141**

14.1. Darf ein Verein ein erweitertes Führungszeugnis von Mitarbeiter*innen verlangen? 141

14.2. Datenschutz im Kleingarten: Vorsicht beim öffentlichen Aushängen von Protokollen 144

15. Zahlen und Fakten **147**

2. Teil: Informationsfreiheitsbericht **153**

1. Vorwort **153**

2. Informationsfreiheit in Deutschland **155**

3. Diese Gerichtsentscheidungen zum Informationsfreiheitsrecht sollten Bürger*innen und Behörden kennen **157**

3.1. IFG NRW kann im Einzelfall auch Zugang zu Verschlusssachen gewähren 157

3.2. Studierende haben Informationsanspruch auch in Bezug auf Prüfungszulassungen 158

3.3. Kommunale Tochterunternehmen unterliegen umfassend dem IFG NRW 158

3.4. Föderale Zusammenarbeit ist weitgehend frei von Informationspflichten nach dem IFG NRW 159

3.5. Anbieter*innen von Rechtsdatenbanken haben keinen Anspruch auf Herausgabe von Gerichtsentscheidungen 159

3.6. Berichte, die auf staatsanwaltschaftlichen Ermittlungen beruhen, sind nicht zugänglich 160

3.7. Ratsmitglieder gehen leer aus 160

4. Aus der Beratungspraxis **161**

4.1 Landtag beschränkt Auskunftsrecht gegenüber öffentlich-rechtlichen Kreditinstituten 161

4.2 Dürfen Behörden die Postanschrift von Bürger*innen verlangen, die Informationen beanspruchen? 164

4.3. Öffentliche Gutachten sind für die Bürger*innen nicht tabu 166

4.4 Nicht jeder Vertrag ist vom Informationszugang ausgenommen 168

4.5 Auch Unternehmen können auskunftspflichtig sein 170

4.6 Gebührenberechnung bei Informationsanträgen: Gute Kommunikation verhindert den Rechtsstreit 173

4.7 Tödlicher Unfall – Behörden müssen schnell informieren 175

4.8 Wer Informationen von einer schwierigen Behörde will, kann es auch mit „Plan B” versuchen 176

4.9 Behörden sollten klar kommunizieren, wenn ihnen begehrte Informationen nicht vorliegen 178

Anhang zum Datenschutzbericht **181**

Veröffentlichungen der Datenschutzkonferenz 2024 **181**

1. Entschließungen der Datenschutzkonferenz 2024 **181**

2. Beschlüsse der Datenschutzkonferenz 2024 **189**

Anhang zum Informationsfreiheitsbericht **215**

Veröffentlichungen der Konferenz der Informationsfreiheitsbeauftragten (IFK) in Deutschland 2023 und 2024 **215**

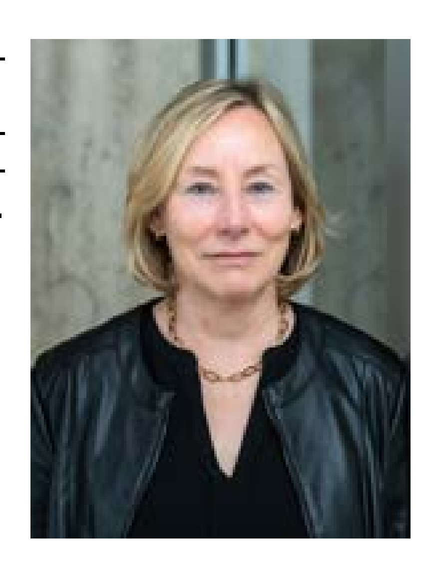
Abkürzungsverzeichnis **223**

Bildnachweise **225**

Impressum **226**

1. Vorwort

Datenschutz ist lästig. Datenschutz ist Täterschutz. Wir brauchen weniger Datenschutz und mehr Datennutzung. Die Datenschutzaufsicht muss zentral vom Bund wahrgenommen werden. Das sind nicht meine Worte. So in etwa lautete die Kritik, die im letzten Jahr wiederholt, auch von Akteur*innen aus Nordrhein-Westfalen, am Datenschutz geübt wurde. Mich hat das gewundert und zugleich auch besorgt. Denn diese Kritik ist nicht nur unberechtigt. Dahinter steckt auch der Versuch, die Axt an dieses bedeutende Freiheitsrecht zu legen.



Bettina Gayk
Landesbeauftragte für Datenschutz und Informationsfreiheit

Zurückstehen soll der Datenschutz meist hinter Sicherheitsbelangen. Das ist die eine Forderung, die zuletzt häufiger von Sicherheitspolitiker*innen und Polizei erhoben wird. Leider zeugt sie von einem offensichtlichen Missverständnis über Sinn und Zweck des Datenschutzes. Datenschutz ist Teil der verfassungsrechtlich garantierten Freiheitsrechte, in die der Staat nur dann eingreifen darf, wenn er gute Gründe dafür geltend machen kann. Kernelement unserer Demokratie ist es, dass staatliche Organe nicht willkürlich die Freiheiten der Bürger*innen beschneiden dürfen. Gerade in einer zunehmend digitalisierten Welt kommt dem Datenschutz eine zentrale Rolle zu, denn er schützt nicht allein Daten um ihrer selbst willen. Geschützt werden die Menschen, um deren Daten es geht. Und diese Menschen sind leicht zu verwunden.

Daten können sehr viel über mich verraten. Neben allgemeinen Meinungen können sich aus Daten politische Ansichten ergeben, sexuelle Neigungen, die Religionszugehörigkeit, Informationen über Krankheiten, Beteiligungen in Vereinigungen, Besitzverhältnisse, berufliche Aktivitäten und vieles mehr. Mittelbar schützt das Recht auf Datenschutz auch weitere Grundrechte, wie etwa die Meinungsfreiheit, die Vereinigungsfreiheit oder die Religionsfreiheit. Nur wer über meine Meinung, meine Religionszugehörigkeit oder meine Mitgliedschaft in einer Vereinigung weiß, kann einen Anlass haben, in diese Rechte einzugreifen. Der Datenschutz ist daher in der digitalen Welt ein ganz zentrales Grundrecht zum Schutz der persönlichen Freiheiten.

Selbstverständlich, auch die Freiheitsrechte gelten nicht schrankenlos. Und gerade die Sicherheit ist ein hohes Gut, das Eingriffe in die Grundrechte einschließlich des Datenschutzes rechtfertigen kann. Genau das

ist es aber, was der Datenschutz von den Verantwortlichen in Regierung und Parlamenten verlangt: eine verfassungskonforme Rechtfertigung. Sie müssen rechtfertigen können, wozu der Staat welche Informationen über die Bürger*innen in welchem Umfang benötigt. Der Staat muss sich auf das beschränken, was zur Erfüllung seiner Aufgaben an Daten erforderlich ist.

Wer also das Zurückstehen des Datenschutzes verlangt, möchte sich möglicherweise diese Rechtfertigung ersparen. Für Regierung und Parlament, das muss an dieser Stelle klar gesagt werden, wäre es aber verfassungswidrig, würden sie sich der Mühe entziehen, sorgsam zwischen den Sicherheitsbelangen und Freiheitsrechten abzuwägen und stattdessen leichtfertig und ungeprüft Eingriffe in die Freiheiten der Bürger*innen erlauben.

Die andere Variante, mit der das Zurückstehen des Datenschutzes verlangt wird, lautet: „Wir brauchen mehr Datennutzung und weniger Datenschutz!" Auch sie verkennt jedoch, dass der Gesetzgeber das existierende Recht fein austariert hat an widerstreitenden Interessen, in diesem Fall von Wirtschaft und Verbraucher*innen.

Um es zu verdeutlichen: Die Datenschutz-Grundverordnung (DS-GVO) setzt in der Europäischen Union den Rechtsrahmen dafür, wie die Rechte von Einzelpersonen, über die Verwendung ihrer Daten grundsätzlich selbst bestimmten zu können, mit der wirtschaftlich motivierten Nutzung in Einklang zu bringen sind. Die Datenschutzaufsichtsbehörden haben das zu kontrollieren. Nach der DS-GVO sind sie verpflichtet, dem Datenschutzrecht Geltung zu verschaffen, wenn die Rechte Einzelner verletzt werden.

Der europäische Gesetzgeber hat damit ein deutliches Signal gesetzt, dass Europa keine Datennutzung nach Wildwest-Manier will, sondern auch im Wirtschaftsverkehr Fairness gelten muss. Diese Idee setzt sich fort in der menschenzentrierten Digitalisierungsinitiative der Europäischen Union. Sie zielt darauf, Datenschutz und Datennutzung zu vereinbaren. Auch hier geht es nicht um ein weniger an Datenschutz, sondern darum, Datennutzung und Datenschutz in einen gerechten Einklang zu bringen.

Nun meinen viele, dass die Datenschutzaufsichten in Deutschland – von denen es in Bund und Ländern insgesamt 18 gibt – zu uneinheitliche Auffassungen hätten. Den kontrollierten Stellen würden daraus Probleme entstehen. Anekdoten, die das belegen sollen, diagnostizieren die Ursache aber unzutreffend. Während meiner inzwischen langen Tätigkeit in der öffentlichen Verwaltung habe ich noch keinen Arbeitsbereich erlebt, in dem länderübergreifend so gezielt daran gearbeitet wird, einheitliche Festlegungen zur richtigen Anwendung des Rechts zu erreichen, wie dies innerhalb der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) der Fall ist.

Die DSK hat längst Strukturen entwickelt, die effektiv zu einheitlichen Positionen führen. Während es für die einheitliche Meinungsbildung des Europäische Datenschutzausschuss (EDSA) gesetzlich Vorgaben in der DS-GVO gibt, hat die DSK das auf nationaler Ebene bestehende Vakuum durch einen Selbstbindungsmechanismus gefüllt. Das heißt: Obwohl wir Aufsichtsbehörden allesamt unabhängige Kontrolleure sind, haben wir vereinbart, uns in bestimmten Fällen an eine einheitliche Entscheidung zu halten. Was hier indessen weiterhin fehlt und gefordert werden sollte, ist die institutionelle Anerkennung der DSK und eine tragfähige Arbeitsstruktur, vergleichbar dem Sekretariat des EDSA.

Was die Kritik zudem verkennt, ist die Tatsache, dass Datenschutz bereits gesetzlich auf Ausgleich widerstreitender Interessen ausgelegt ist sowie darauf, die Datenverarbeitung auf das für den jeweiligen Zweck Erforderliche zu beschränken. Das ist je nach Lebensbereich und je nach Sachlage sehr individuell gestaltet. Zudem sind auch die technischen Rahmenbedingungen der Stellen, die die Daten verarbeiten, ganz unterschiedlich – was aber eine Rolle spielt bei der Frage, ob der Datenschutz eingehalten ist. Vereinfacht gesagt, schüren Kritiker*innen die Erwartung, man könne für ganz individuell gestaltete Sachverhalte einheitliche rechtliche Lösungen zentral anbieten. Das ist nicht der Fall. Man kann jedoch in wichtigen Fragen durch Selbstbindung ein kollektives Zusammenwirken erreichen.

Diese dezentrale, aber in wichtigen Fragen kollektive Aufsichtsstruktur hat erhebliche Vorteile für Unternehmen wie für die Bürger*innen im jeweiligen Bundesland. Seit Inkrafttreten der DS-GVO erreichen uns in NRW rund 12.000 Anfragen jährlich. Vor allem die Menschen, die von einer Datenverarbeitung betroffen sind, haben ganz individuelle Probleme mit ihrem Arzt, mit ihrer Rechtsanwältin, mit dem Unternehmen, bei dem sie beschäftigt sind oder mit einer Auskunftei, die Daten über sie weitergegeben hat, um nur einige Felder zu nennen. Aber auch Unternehmen, Verbände und Vereine suchen unseren Rat. Wir sind hier nah dran, an den Unternehmen ebenso wie an den Betroffenen, und können ganz oft vermitteln. Wir stehen im Erfahrungsaustausch mit der Wirtschaft hierzulande, um eine rechtskonforme Datenverarbeitung zu fördern. Das kann durch eine zentralisierte Datenschutzaufsicht in gleicher Weise nicht geleistet werden.

Und noch etwas will ich in diesem Zusammenhang erwähnen: Ich beobachte mit zunehmendem Unbehagen, dass es nicht nur bei der Datenschutzaufsicht einen Trend zur Zentralisierung gibt, sondern auch in anderen Sachbereichen. Dies wird durch die eher französisch zentral orientierte Verwaltung in Europa befördert und untergräbt so schleichend unsere traditionell föderale Struktur in Deutschland. Ich bin davon überzeugt, dass Zentralisierung aber kein Allheilmittel ist. Unser Land hat im Gegenteil mit dezentralen Strukturen in der Vergangenheit

gute Ergebnisse erzielt, weil die föderale Verwaltung einen unmittelbareren Einblick in die Problemstellungen vor Ort hat.

Welche dieser Problemstellungen uns im vergangenen Jahr beschäftigt haben, finden sie in Auszügen in diesem Bericht. Sie sind gute Beispiele dafür, dass Datenschutz eben nicht lästig ist, sondern notwendig. Dass er nicht Täterschutz ist, sondern gut abgewogen die Freiheit schützt. Und dass Datenschutz und Datennutzung in fairem Einklang miteinander stehen. Ich erhoffe mir Unterstützung im Land, dass wir diese erfolgreiche Arbeit – auch in der Aufsicht über den privaten Bereich – unverändert fortsetzen können.

Bettina Gayk
Frühjahr 2025

2. Datenschutz in Europa



Der Europäische Datenschutzausschuss (EDSA) soll die einheitliche Anwendung der Datenschutz-Grundverordnung und der EU-Datenschutz-Richtlinie im Bereich von Justiz und Inneres in der Europäischen Union sicherstellen. Dazu verfügt er über ein eigenes Sekretariat in Brüssel und ist von der EU unabhängig. Der EDSA setzt sich aus den Leiter*innen aller Aufsichtsbehörden im Europäischen Wirtschaftsraum sowie dem Europäischen Datenschutzbeauftragten zusammen. Gemeinsame Vertreterin für die deutschen Datenschutzbehörden im EDSA ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Ihr Stellvertreter in diesem Ausschuss ist der Bayerische Landesbeauftragte für den Datenschutz.

Der EDSA erstellt unter anderem Leitlinien zu wichtigen datenschutzrechtlichen Fragen sowie Stellungnahmen und trifft insbesondere verbindliche Entscheidungen.

Der EDSA wird bei seiner Arbeit von mehreren Fachuntergruppen (Expert Subgroups – ESG) unterstützt, in denen auch die nationalen Aufsichtsbehörden vertreten sind. Die LDI NRW ist in den Expert Subgroups

- Key Provisions (rechtliche Grundsatzfragen),
- Compliance, E-Government & Health (CEH) (Regelkonformitätsverfahren, digitale Verwaltung und Gesundheitsbereich),
- Financial Matters (Finanzangelegenheiten einschließlich Banken und Kreditwirtschaft) und
- Technology (technischer Datenschutz)

aktiv und vertritt dort die deutschen Aufsichtsbehörden.

Strategie und Arbeitsprogramm

Die Ziele seiner Arbeit hat der EDSA in seiner Strategie für 2024 bis 2027 festgelegt, und dabei die wichtigsten Maßnahmen benannt:

1. **Säule:** Verbesserung der Harmonisierung und Förderung der Einhaltung
2. **Säule:** Stärkung einer gemeinsamen Durchsetzungskultur und der wirksamen Zusammenarbeit
3. **Säule:** Schutz des Datenschutzes in der sich entwickelnden digitalen und aufsichtsübergreifenden Landschaft
4. **Säule:** Beitrag zum globalen Datenschutzdialog

Der besondere Fokus liegt auf dem Zusammenspiel mit dem digitalen Regulierungsrahmen der EU (Europäische Datenstrategie). Neue digitale Gesetze, wie etwa der Digital Services Act (DSA), haben Auswirkungen auf den Datenschutz. Hier soll mit anderen Regulierungsbehörden zusammengearbeitet werden, um das Recht auf Datenschutz in die allgemeine Regulierungsarchitektur einzubetten.

Das erste EDSA-Arbeitsprogrammen für die Jahre 2024 und 2025 soll die Strategie umsetzen. Es ist auf der Website des EDSA www.edpb.europa.eu abrufbar. Die ersten selbst gestellten Aufgaben wurden dabei bereits erfüllt.

So sollen zur Verbesserung der Harmonisierung und Förderung der Einhaltung (1. Säule) Leitlinien und Werkzeuge für ein breiteres Publikum zu einer Reihe von Themen bereitgestellt werden. Besonders in den Blick genommen werden dabei Personen ohne besondere Datenschutz-Fachkenntnisse, kleine und mittlere Unternehmen sowie Einzelpersonen – einschließlich besonders schutzbedürftiger Menschen.

In diesem Sinne erläutert etwa die im Oktober 2024 veröffentlichte „Leitlinie zur auf Art. 6 (1) (f) gestützten Datenverarbeitung" eine wichtige Rechtsgrundlage für Datenverarbeitung durch Unternehmen. Sie gibt eine detaillierte Anleitung, wie die Abwägung zwischen dem berechtigten Interesse an einer Datenverarbeitung durch ein Unternehmen und den Rechten und Interessen der von der Verarbeitung betroffenen Personen durchgeführt werden sollte. Auf das Anwendungsfeld der Verarbeitung von Kinderdaten wird dabei in der Leitlinie besonders eingegangen. Die LDI NRW hat intensiv an der Leitlinie mitgewirkt. Sie stellt die deutsche Ländervertreterin in der Arbeitsgruppe des EDSA, die die Leitlinie erarbeitet hat. Siehe hierzu unter 10.1.

Weitere Leitlinien werden unter Mitarbeit der LDI NRW derzeit bearbeitet, so etwa Leitlinien zur Verarbeitung personenbezogener Daten von Kindern. Diese nimmt die besonderen Bedürfnisse und Interessen von Kindern bei der Anwendung des Datenschutzrechts in den Blick, insbesondere bei der Erfüllung von Informationspflichten und bei der Wahrnehmung ihrer Betroffenenrechte. Weiterer Schwerpunkt sind technische Aspekte wie Altersverifizierung und spezielle datenschutzfreundliche Gestaltung von Webangeboten.

Pur-Abo-Modelle

Nach den deutschen Aufsichtsbehörden beschäftigt sich nun auch der EDSA mit der Rechtmäßigkeit von Pur-Abo-Modellen auf Websites. Dabei haben die Nutzer*innen die Wahl, ob sie einen zahlungspflichtigen Abo-Vertrag abschließen oder ihre Zustimmung zum Tracking erteilen möchten. Die erste EDSA-Stellungnahme „Wirksame Einwilligung im Kontext von Pur-Abo-Modellen, die von großen Online-Plattformen umgesetzt werden" bezieht sich allerdings vorerst nur auf große Online-Plattformen. Siehe hierzu unter 11.1. Der EDSA entwirft derzeit Leitlinien, die einen weiteren Anwendungsbereich haben und sich auf alle Websitebetreiber*innen mit Pur-Abo-Modellen beziehen.

Kriterien für ein Datenschutz-Zertifikat

2024 hat der EDSA zum zweiten Mal europaweit gültige Kriterien für eine Datenverarbeitungszertifizierung genehmigt. Diesem Verfahren vorausgegangen war die Genehmigung der nationalen Zertifizierungskriterien in Deutschland durch die LDI NRW.

Viele Unternehmen oder Behörden lassen sich bei ihrer Datenverarbeitung durch sogenannte Auftragsverarbeiter unterstützen. Darunter fallen beispielsweise die Dienste eines Rechenzentrums oder ausgelagerte Clouddienste. Ob diese Dienste datenschutzkonform sind, ist für diejenigen, die sie nutzen wollen, oft nicht leicht zu beurteilen. Ein Zertifikat vereinfacht eine solche Beurteilung.

Dies gilt auch für das Zertifikat „European Privacy Seal" (EuroPriSe), das den Datenschutz in Europa verbessern soll. Unternehmen in Europa sollen damit künftig belegen können, dass die Art und Weise, wie sie Daten im Auftrag anderer Unternehmen verarbeiten, den Anforderungen des europäischen Datenschutzrechts entspricht. Der EDSA hat 2024 die europaweit gültigen Kriterien für diese Zertifizierung genehmigt und

damit zum zweiten Mal einen solchen Schritt vollzogen. Dabei handelt es sich um eine Fortentwicklung der bereits im Oktober 2022 genehmigten nationalen Kriterien zur Zertifizierung von Auftragsverarbeitern eines in NRW ansässigen Unternehmens durch die LDI NRW.

Eine Zertifizierung bedeutet – ganz allgemein – eine Begutachtung durch unabhängige Fachleute, die den Verarbeitungsvorgang personenbezogener Daten analysieren und auf Normgerechtigkeit prüfen. In einem „Konformitätsbewertungsprogramm" sind Kriterien und Methoden für die Begutachtung festgelegt. Dieses Programm muss – so sieht es die DS-GVO vor – der Aufsichtsbehörde zur Beurteilung und Genehmigung vorgelegt werden. Im Falle europäischer Zertifizierungskriterien genehmigt der EDSA die Kriterien selbst. Mit seiner Entscheidung zum „European Privacy Seal" hat der EDSA zugleich die Einschätzung der LDI NRW bestätigt. Die EDSA-Entscheidung hat zur Folge, dass die Kriterien nun von allen Aufsichtsbehörden EU-weit anerkannt werden.

3. Datenschutz in Deutschland



Die Aufsichtsbehörden in Deutschland stimmen sich in der Datenschutzkonferenz (DSK) ab. 2024 führte die überraschende Ernennung der Leiterin der Datenschutzaufsichtsbehörde in Bremen zur Präsidentin des dortigen Rechnungshofs zu einem mehrfachen Wechsel im Vorsitz. Nach dem planmäßigen Vorsitz durch Bremen, übernahm kurzzeitig noch einmal der Vorjahresvorsitz Schleswig-Holstein und dann Hessen den Vorsitz. Getagt wurde unter anderem in Bremerhaven und Wiesbaden.

Die DSK hat eine zentrale Rolle für die einheitliche Anwendung des Datenschutzrechts in Deutschland. Nach der DS-GVO leistet jede Aufsichtsbehörde einen Beitrag zur einheitlichen Anwendung der Verordnung. Der Europäische Datenschutzausschuss (EDSA) als Gremium soll diese Einheitlichkeit in bestimmten Fällen zwischen den europäischen Mitgliedstaaten herstellen. Bisher nimmt die DSK ähnliche Aufgaben für die innerdeutsche Abstimmung zwischen den Datenschutzaufsichtsbehörden des Bundes und der Länder in grundsätzlichen Fragen informell wahr. Ein Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes, der vor der vorgezogenen Bundestagswahl aber nicht mehr verabschiedet wurde, sollte die DSK institutionalisieren, um der nationalen Koordinierung erstmalig den notwendigen gesetzlichen Rahmen zu geben.

Die DSK hat sich in ihrer Geschäftsordnung Regelungen auferlegt, die verbindliche Mehrheitsentscheidungen in Fragen der Rechtsanwendung ermöglichen. In Beschlüssen, Kurzpapieren, Anwendungshinweisen und Orientierungshilfen

richtet sich die DSK an für die Datenverarbeitung Verantwortliche und gibt ihnen Hinweise für die richtige Rechtsanwendung. Die Inhalte dieser Papiere legen die Datenschutzaufsichtsbehörden ihrer eigenen Aufsichtsarbeit zugrunde. Für Reaktionen auf datenschutzpolitische Entwicklungen nutzt die DSK in der Regel das Format der Entschließung. Sie erzielt mit dieser Arbeit homogene Ergebnisse und stellt eine einheitliche Datenschutzaufsicht in Deutschland sicher. Fast ritualartig erhobene Klagen aus Teilen der Digitalwirtschaft über eine uneinheitliche Datenschutzaufsicht können sich insofern nur auf längst vergangene Zeit beziehen.

Die DSK hat zur Unterstützung ihrer Arbeit Arbeitskreise eingerichtet. Über unsere Vorsitze der Arbeitskreise wurden mehrere fachliche Impulse an die DSK geleitet. Im Rahmen der DSK leitet die LDI NRW die Arbeitskreise

- Wirtschaft,
- Statistik,
- Kreditwirtschaft sowie
- Adresshandel und Werbung (gemeinsam mit dem Bayerischen Landesamt für Datenschutzaufsicht).

Diese Facharbeitskreise stehen im Austausch mit Wirtschaft und Verwaltung. Sie können Vertreter*innen der Wirtschaft aus diesen Bereichen oder Expert*innen etwa aus Verbänden oder anderen Behörden zu Sitzungen einladen. Ihre Ergebnisse, die sie der Konferenz zur Entscheidung vorlegen, prüfen sie bei Bedarf durch Anhörungen von Interessenvertretungen oder auch der Allgemeinheit. Darüber hinaus nutzt die Konferenz die Facharbeitskreise, wenn aus Verwaltung und Wirtschaft Fragen zu Klärung an sie herangetragen werden, um zeitnahe Rückmeldungen geben zu können. Über eine Vernetzung der nationalen Facharbeitskreise mit den Fachuntergruppen des EDSA ist Deutschland auch in Europa schnell und einheitlich sprachfähig.

Veröffentlichungen der DSK

Die Beschlüsse und Entschließungen des Jahres 2024 sind im Anhang abgedruckt und mit weiteren Veröffentlichungen auch auf der Website der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

Besonders hinzuweisen ist dabei auf die Orientierungshilfen zu funkbasierten Zählern und zur Künstlichen Intelligenz sowie auf die Entschließung zur menschenzentrierten Digitalisierung in der Daseinsvorsorge:

Smart Metering: Neue Orientierungshilfe hilft im Umgang mit funkbasierten Strom-, Heizungs- und Wasserzählern

Die unter der Federführung der LDI NRW erstellte Orientierungshilfe beantwortet Fragen im Zusammenhang mit der Rechtmäßigkeit der funkgesteuerten Erhebung und Übermittlung von Verbrauchsdaten. Ziel ist es, den technischen Fortschritt zu unterstützen – ohne dass der Datenschutz zu kurz kommt. Siehe hierzu unter 12.2.

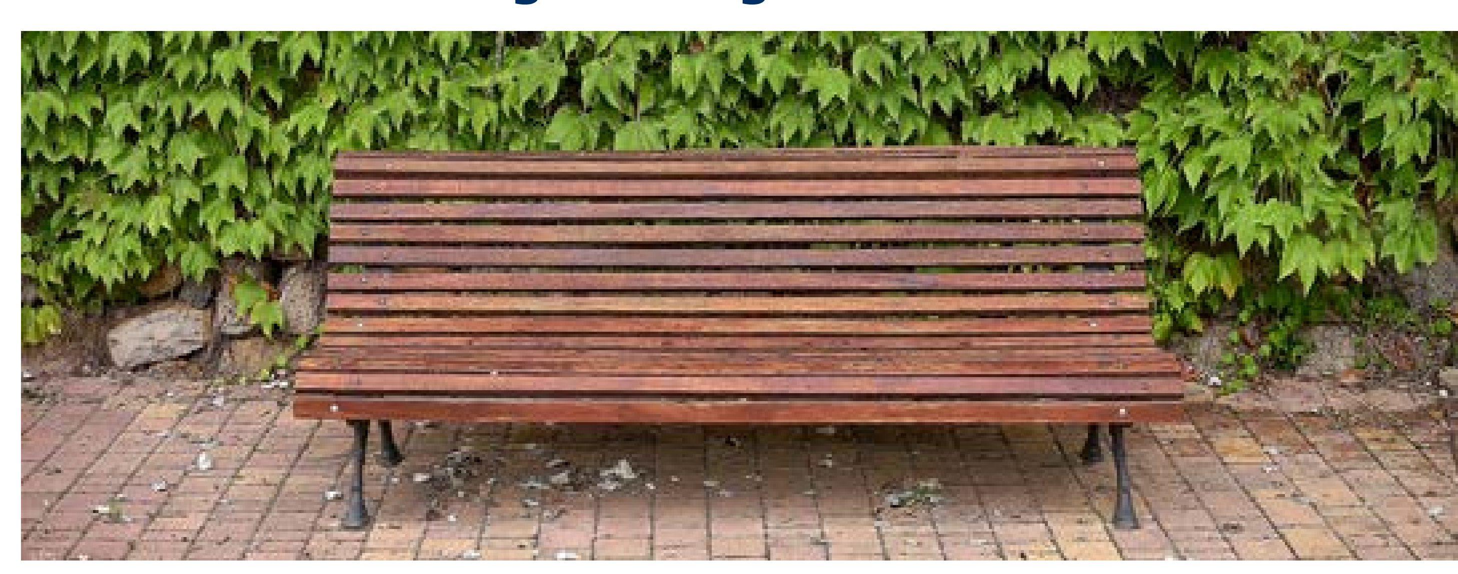
Orientierungshilfe „Künstliche Intelligenz und Datenschutz”

Zusammen mit anderen Aufsichtsbehörden hat die LDI NRW die Orientierungshilfe „Künstliche Intelligenz und Datenschutz” erstellt. Sie gibt Antworten auf die Frage, unter welchen Voraussetzungen KI-Anwendungen datenschutzkonform eingesetzt werden dürfen. Oft kommt es bei der Nutzung dieser Systeme zu einer Verarbeitung personenbezogener Daten, sodass die DS-GVO Anwendung findet und deren Regeln zu beachten sind. Siehe hierzu unter 5.1.

Menschenzentrierte Digitalisierung in der Daseinsvorsorge

Die Entschließung „Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen!” nimmt die datenschutzrechtlichen Fragen zu ausschließlich digital angebotenen daseinsvorsorgerelevanten Dienstleistungen in den Blick. Gemeint ist etwa, dass Zugtickets oder der Kontakt zu Energieversorgungsunternehmen künftig nur noch digital angeboten werden könnten. Die Fragen hierzu und ihre Antworten wurden in einer Arbeitsgruppe aufbereitet, an der sich auch die LDI NRW beteiligt hat. Derzeit geht der Trend dahin, Bürger*innen in eine rein digitale Welt zu drängen. Der Gesetzgeber muss hier das Interesse an allgemeiner Teilhabe an der Daseinsvorsorge gegen die unternehmerische Freiheit zu ausschließlich digitalen Angeboten abwägen. Siehe hierzu unter 6.1.

4. Änderung des Bundesdatenschutzgesetzes darf nicht auf die lange Bank geschoben werden



Die Überarbeitung des wichtigen BDSG kommt nicht voran. Zwar hat die Bundesregierung 2024 einen Änderungsentwurf vorgelegt. Doch die deutschen Datenschutzaufsichtsbehörden sehen noch erhebliches Verbesserungspotenzial. Nun ist es an der neuen Regierung, die Neuregelung zügig anzugehen. Es besteht Handlungsbedarf.

Die Datenschutzkonferenz, kurz DSK, hat eine wichtige Rolle bei der einheitlichen Anwendung des Datenschutzrechts in Deutschland. In ihr haben sich die Datenschutzaufsichtsbehörden von Bund und Ländern zusammengeschlossen, um ihre Koordinierung und Zusammenarbeit zu fördern. Dabei sind die Erwartungen an die DSK im Laufe der Jahre immer weiter angewachsen – nicht zuletzt, weil die europäische Rechtsentwicklung eine immer intensivere und schnellere Zusammenarbeit erfordert.

Mit der Änderung des BDSG wollte die Bundesregierung gemäß Vereinbarungen des Koalitionsvertrags diese Entwicklung aufgreifen und die DSK im BDSG verankern. Außerdem sollten nach einer Untersuchung der Wirkungen des BDSG weitere Änderungen des Gesetzes erfolgen, insbesondere mit Blick auf die bessere Durchsetzung und Abstimmung des Datenschutzes. Allerdings blieb der dazu vorgelegte Gesetzentwurf hinter den Erwartungen der DSK – und damit auch der LDI NRW – zurück. Am Ende konnte das Gesetzgebungsverfahren vor der Neuwahl des Bundestags nicht abgeschlossen werden. Insofern besteht für das neue Parlament und die neue Regierung dringender Handlungsbedarf.

Berücksichtigt werden sollten dabei zahlreiche Optimierungsbedarfe. Zwar wurde die DSK immerhin im Gesetzentwurf genannt. Aber für

eine Unterstützung durch eine eigene Geschäftsstelle, wie von der DSK gefordert, gab es keine Anzeichen. Hinzu kommen weitere notwendige Änderungen, auf die die DSK die Bundesregierung aufmerksam gemacht hat, abrufbar unter www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf.

So hatten etwa die Aufsichtsbehörden schon 2023 Regelungen zum sog. Scoring empfohlen. Scoring wird durch Wirtschaftsauskunfteien wie die SCHUFA eingesetzt. Mit diesem Verfahren soll die Bonität von Verbraucher*innen oder Unternehmen ermittelt werden, die dann mit einer Note auf einer Ratingskala ausgedrückt wird. Diese Vorschläge wurden von der Bundesregierung im Gesetzentwurf erfreulicherweise auch zum Teil aufgegriffen. Allerdings bleibt noch Verbesserungsbedarf. Klarere Definitionen zum Beispiel würden die Regelungen rechtssicherer machen. Diskriminierungsverbote sollten zudem ausschließen, dass Alter und Geschlecht bei der Beurteilung der Kreditwürdigkeit berücksichtigt werden. Darüber hinaus fehlt es an Regelungen zu Verfahren, die die Richtigkeit und Aktualität der Daten für das Scoring sicherstellen. Zwar sollten wissenschaftlich anerkannte, mathematisch-statistische Verfahren zugrundgelegt werden. Um dies operabel zu halten, müsste aber zugleich auch normiert werden, dass ein solches Verfahren durch eine Zertifizierung bestätigt werden muss. Weiter sollten Informationen über die Scoring-Kriterien der betroffenen Person proaktiv mitgeteilt werden und das Ziel berücksichtigen, dass die Person eine Entscheidung mit den maßgeblichen Informationen anfechten kann. Schließlich fehlt es bisher an der Pflicht, die betroffene Person verständlich und getrennt von anderen Informationen über ihre Rechte zu informieren.

Mit Blick auf den vorgelegten Gesetzesentwurf zum Scoring bei der Kreditwürdigkeitsprüfung hatte die DSK empfohlen, diesen Gesetzesvorschlag durch eine Sachverständigenanhörung umfassend zu analysieren, um Kritik auszuräumen und Rechtssicherheit zu schaffen. Es sollte etwa vertieft geprüft werden, inwieweit hier im nationalen Recht überhaupt Gestaltungsspielraum in der gewählten Rechtskonstruktion besteht.

Der Gesetzentwurf zur Änderung des BDSG sieht außerdem problematische Zuständigkeitsregeln vor. So soll in bestimmten Fällen, in denen etwa Unternehmen gemeinsam für eine Datenverarbeitung verantwortlich sind, die jeweils der Datenschutzaufsicht verschiedener Behörden unterliegen, nur eine einzige Behörde zuständig werden, wenn diese Konstellation den Behörden angezeigt wird. Das Ziel einer solchen Regelung ist nachvollziehbar, da sie die einheitliche und effektive Rechtsdurchsetzung stärken würde. Die Umsetzung im Entwurf ist aber misslungen. Denn dadurch entsteht potenziell mehr Rechtsunsicherheit, weil bereits Streit über die Zuständigkeit selbst entstehen kann. Insbesondere kann die schlichte Behauptung der Unternehmen, es läge eine gemeinsame Verantwortlichkeit vor, nicht entscheidend sein. Die betroffenen Aufsichts-

behörden müssen dieses Tatbestandsmerkmal anhand der Tatsachenlage überprüfen können, was bisher nicht vorgesehen ist.

Hinzu kommt, dass Unternehmen ein sog. „Forum-Shopping" erlaubt würde, das heißt, dass Unternehmen auswählen können, welche Behörde sie kontrollieren soll. Es sollte deswegen nicht auf die Anzeige und Wahl durch das Unternehmen ankommen, sondern auf objektive Kriterien und eine Prüfung durch die Behörden. Ganz grundsätzlich ist auch zu fragen, ob eine solche Regelung, die etwa für Unternehmen ein Vorteil wäre, für die betroffenen Personen unschädlich ist.

Schließlich muss klarer geregelt werden, wie bestimmte Religionsgemeinschaften datenschutzrechtlich einzuordnen sind. Und die Neuregelung sollte auch dazu genutzt werden, Defizite bei den Mitteln zur Rechtsdurchsetzung durch die Aufsichtsbehörden zu beseitigen.

Fazit

Der Entwurf für eine Neuregelung des BDSG enthielt zwar einige kritische Punkte, hatte aber auch das Potenzial, mehr Rechtssicherheit zu schaffen und die Verbindlichkeit der Zusammenarbeit der Aufsichtsbehörden zu stärken. Der neue Bundestag und die neue Bundesregierung sollten das begonnene Vorhaben wieder aufgreifen und in den von der DSK aufgezeigten Punkten verbessern.

5. Künstliche Intelligenz



5.1. Künstliche Intelligenz und der Datenschutz: Was Verantwortliche beachten sollten

Der Einsatz Künstlicher Intelligenz (KI) nimmt rasant zu, das Angebot an KI-Systemen wächst stetig. Werden dort personenbezogene Daten verarbeitet, müssen sich die Verantwortlichen fragen, unter welchen Voraussetzungen sie die KI-Anwendung datenschutzkonform einsetzen können. Die deutschen Datenschutzbehörden haben dazu nun eine Orientierungshilfe herausgegeben.

Mit ChatGPT fing es an – und seither hört der Hype um die KI nicht mehr auf. Mittlerweile existiert ein breites Angebot an verschiedenen KI-Systemen, die für verschiedenste Zwecke eingesetzt werden können. Mögliche Kund*innen und damit Anwendende für diese Systeme sind sowohl öffentliche als auch private Stellen. Besonderes Interesse gilt dabei den sog. Large-Language-Models (LLM) wie ChatGPT, welche häufig im Zusammenhang mit Chatbots eingesetzt werden. Aber das ist keineswegs alles: Die Anwendungsfälle nehmen stetig zu, von der Zusammenfassung von Texten bis hin zur Sortierung von Posteingängen.

Nicht selten kommt es bei der Nutzung dieser Systeme auch zu einer Verarbeitung personenbezogener Daten, und dann muss die DS-GVO beachtet und eingehalten werden. Insbesondere eine Frage steht dabei im Mittelpunkt: Wie können die für die Datenverarbeitung Verantwortlichen das KI-System datenschutzkonform für den beabsichtigten Zweck einsetzen?

Hilfestellung bei der Beantwortung geben nun die Landesdatenschutzaufsichtsbehörden. Zusammen mit den anderen Aufsichten hat die LDI NRW die Orientierungshilfe „Künstliche Intelligenz und Datenschutz" entwickelt, abrufbar unter www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf. Zwar liegt der Schwerpunkt der Veröffentlichung auf den LLM und darauf basierenden Systemen. Aber viele der in dem veröffentlichten Papier angestellten Erwägungen sind auch für weitere KI-Systeme relevant.

In Form einer Checkliste formuliert die Orientierungshilfe Fragen, die sich datenschutzrechtlich Verantwortliche bei der Konzeption des Einsatzes, der Auswahl, der Implementierung und der Nutzung von KI-Systemen stellen und die sie beantworten müssen. Dabei geht es insbesondere um die Grundsätze der Verarbeitung personenbezogener Daten (etwa Zweckbindung, Transparenz und Richtigkeit) sowie die Gewährleistung der Ausübung von Betroffenenrechten. Zu den einzelnen Punkten werden zudem praxisnahe Beispiele gegeben, um die Problemstellung und die mögliche Lösung zu veranschaulichen.

Auch wenn die Adressat*innen des Papiers vorrangig die Anwendenden von KI-Systemen sind, richtet es sich mittelbar auch an Entwickelnde und Herstellende von KI-Systemen. Denn sie müssen die Anforderungen technisch umsetzen, um einen datenschutzkonformen Einsatz durch die Anwendenden anhand der Kriterien der Orientierungshilfe zu ermöglichen.

Die DSK erstellt darüber hinaus derzeit eine Handreichung zu technischen und organisatorischen Maßnahmen für KI-Anwendungen, die sich direkt an Entwickelnde und Herstellende richtet. Gemäß den Prinzipien Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sollten die datenschutzrechtlichen Anforderungen so früh wie möglich im Lebenszyklus der KI-Systeme berücksichtigt werden.

Fazit

Bevor KI-Systeme eingesetzt werden, müssen sich Anwendende kritisch mit den datenschutzrechtlichen Anforderungen auseinandersetzen. Unter Umständen sind ergänzende technische oder organisatorische Maßnahmen erforderlich. Insbesondere sollte ein Augenmerk darauf gelegt werden, dass die Betroffenenrechte wahrgenommen werden können und personenbezogenen Daten von Betroffenen nicht ohne Rechtsgrundlagen verarbeitet werden.

5.2. Die neue EU-Verordnung über künstliche Intelligenz: Einige Probleme müssen noch gelöst werden

Ab 2025 gelten neue Vorgaben für den Einsatz von Künstlicher Intelligenz. Dazu wurde von der EU die KI-VO geschaffen. Doch es bleiben Rechtsunsicherheiten, vor allem im Zusammenspiel mit der DS-GVO. Und noch eine Frage ist unbeantwortet: Wie muss damit umgegangen werden, wenn Markt- und Datenaufsicht zwei verschiedenen Behörden zugewiesen werden?

Es war eine schwierige Geburt, doch Mitte letzten Jahres war es dann soweit: die Mitgliedstaaten der EU konnten sich auf eine KI-VO verständigen. Sie stellt umfassende Regeln für das Inverkehrbringen, die Inbetriebnahme und die Verwendung Künstlicher Intelligenz auf, um die Einhaltung der Grundrechte zu gewährleisten und gleichzeitig Innovation zu fördern. Gelten soll die KI-VO vor allem für „Anbieter" von KI-Systemen, die in der EU in Verkehr gebracht oder in Betrieb genommen werden, sowie für Betreiber dieser Systeme, die ihren Sitz in der EU haben oder sich in der EU befinden.

Sie stellt umfassende Regeln für die Anwendung von KI-Systemen auf, um die Einhaltung der Grundrechte zu gewährleisten und gleichzeitig Innovation zu fördern. Gelten soll die KI-VO vor allem für Anbieter, Importeur*innen oder Händler*innen von KI-Systemen, die in der EU in Verkehr gebracht werden, sowie für Betreibende dieser Systeme, die ihren Sitz in der EU haben oder deren KI-Systeme in der EU verwendet werden.

Eine Überprüfung der neuen Vorschriften zeigt jedoch, dass es in der praktischen Anwendung zu Problemen kommen kann, insbesondere im Zusammenspiel mit der DS-GVO. Die LDI NRW hat sich 2024 mit diesem Spannungsfeld befasst und einige wichtige Punkte herausgearbeitet.

So ergeben sich schon wegen der unterschiedlichen Begrifflichkeiten in den beiden Rechtsakten unterschiedliche Adressat*innenkreise. Die DS-GVO kennt lediglich den „Verantwortlichen" und den „Auftragsverarbeiter". Verantwortlicher nach Art. 4 Nr. 7 DS-GVO ist, wer alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Primäre Adressat*innen der KI-VO sind dagegen die das KI-System entwickelnde und auf den Markt bringende „Anbieter" – mit der Verantwortung für die rechtmäßige Entwicklung des KI-Systems. Außerdem benennt die KI-VO den das KI-System zum Einsatz bringenden „Betreiber" – mit der Verantwortung für den rechtmäßigen Einsatz des KI-Systems.

Die Hauptpflichten obliegen nach der KI-VO dem Anbieter des KI-Systems und nach der DS-GVO in der Regel dem Betreiber als Verantwortlichen

für die Verarbeitung der Daten mittels des KI-Systems. Im Sinne der DS-GVO können einsatzabhängig auch Nutzende und Anbieter ggf. in gemeinsamer Verantwortlichkeit mit Betreibern verantwortlich sein.

Über diese Schwierigkeiten hinaus ergeben sich Fragen bei der Feststellung der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Denn die KI-VO führt zwei neue Tatbestände ein, welche die Verarbeitung personenbezogener Daten für bestimmte Zwecke erlauben.

Zum einen ist da Art. 59 Abs. 1 KI-VO, der die Weiterverarbeitung personenbezogener Daten bei der Tätigkeit in einem KI-Reallabor vorsieht – und dabei den datenschutzrechtlichen Grundsatz der strengen Zweckbindung nach Art. 5 Abs. 1 Buchstabe b DS-GVO durchbricht. Nach dem Wortlaut der neuen Norm wird die Weiterverarbeitung von „rechtmäßig für andere Zwecke erhobene(n) personenbezogene(n) Daten […] für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme" in Reallaboren erlaubt, ohne dass die Voraussetzungen des Art. 5 Abs. 1 Buchstabe b DS-GVO geprüft werden müssen. Dabei ist allerdings zu berücksichtigen, dass Art. 59 Abs. 1 KI-VO lediglich für KI-Systeme gilt, die für bestimmte Einsatzzwecke entwickelt werden, und unter der Voraussetzung, dass zusätzliche technische Sicherheitsvorkehrungen eingehalten werden. So ist die Anwendung der neuen Rechtsgrundlage nach Art. 59 Abs. 1 Buchstabe a KI-VO auf die Entwicklung solcher innovativer KI-Systeme beschränkt, die einem erheblichen öffentlichen Interesse dienen, zum Beispiel in den Bereichen der öffentlichen Sicherheit und Gesundheit oder dem Umweltschutz.

Außerdem gilt die neue Vorschrift des Art. 59 Abs. 1 Buchstabe b KI-VO weiterhin nur für solche Datenverarbeitungen, die für die Erfüllung der technischen Anforderungen an Hochrisiko-KI-Systeme erforderlich sind, und „sofern diese Anforderungen durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten nicht wirksam erfüllt werden können." Der Anbieter hat weiterhin sicherzustellen, dass die Erhebung der Daten rechtmäßig erfolgte.

Neben Art. 59 Abs. 1 KI-VO gibt es zum anderen nun auch Art. 10 Abs. 5 KI-VO. Diese Norm stellt eine Durchbrechung des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten durch den Anbieter dar (Art. 9 Abs. 2 Buchstabe g DS-GVO). Danach kann der Anbieter rechtmäßig erhobene Daten auch zur „Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen" einsetzen, sofern dies „unbedingt erforderlich ist" und angemessene Vorkehrungen zum Schutz der Betroffenen-Grundrechte etwa durch Pseudonymisierungen oder Verschlüsselungen getroffen werden.

Ansonsten enthält die KI-VO keine weiteren Regelungen, die die Verarbeitung von personenbezogenen Daten gemäß der DS-GVO in den verschiedenen Lebenszyklen eines KI-Systems modifizieren. Die Ver-

arbeitung solcher Daten im KI-Kontext unterliegt daher – außerhalb der KI-Reallabore nach der KI-VO – weiterhin den Rechtsgrundlagen der DS-GVO. Hier ist insbesondere die einzelfallabhängige Abwägung zwischen den Interessen des Verantwortlichen oder eines Dritten und denjenigen der betroffenen Person zu nennen (nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO).

Sofern es um technische und organisatorische Maßnahmen geht, gibt es zudem Schnittmengen zwischen der DS-GVO und der KI-VO. Im Rahmen des konkreten Einsatzes des KI-Systems erlangt beispielsweise die notwendige, durch den Betreiber durchzuführende Grundrechte-Folgenabschätzung eine besondere Bedeutung (Art. 27 KI-VO). Sie hat als Ergänzung zur Datenschutz-Folgeabschätzung nach Art. 35 DS-GVO neben anderen Grundrechten auch spezifische Risiken für die informationelle Selbstbestimmung betroffener Personen in den Blick zu nehmen.

Die KI-VO stellt darüber hinaus auch weitere Anforderungen an die Entwicklung von Hochrisiko-KI-Systemen auf, die ihrerseits datenschutzrechtliche Kernanliegen teilen und deren effektive Umsetzung damit zugleich eine Stärkung der datenschutzrechtlichen Grundprinzipien nach Art. 5 Abs. 1 DS-GVO begründet. Dies gilt vor allem für die Implementierung eines allgemeinen Risikomanagements und die Durchführung eines Daten-Governance-Verfahrens (nach Art. 9 und 10 KI-VO) sowie für die hinreichende Aufzeichnung, Transparenz, menschliche Beaufsichtigung und Robustheit des Lernverfahrens (Art. 12 bis 15 KI-VO). Für die Adressat*innen von DS-GVO und KI-VO hätte eine Bündelung der Folgenabschätzungsverfahren Synergien schaffen können und einiges erleichtert. Das wurde bisher bei den europäischen Rechtsakten vernachlässigt.

Beim Blick in die Zukunft gilt es nun, auf nationaler Ebene vor allem die Behörden festzulegen, die die Aufsicht nach der KI-VO führen sollen. Denn hier ist die Zuständigkeit teilweise noch ungeklärt oder wirft Fragen auf.

Teils ergeben sich Festlegungen bereits aus dem Verfassungsrecht und konkret aus Art. 74 Abs. 8 in Verbindung mit Anhang III Nr. 1, 6, 7 und 8 KI-VO. Danach sind die Datenschutzaufsichtsbehörden der Länder als Marktüberwachungsbehörden jedenfalls für solche Hochrisiko-KI-Systeme zu benennen, die von der öffentlichen Verwaltung auf Länderebene eingesetzt werden sollen. Dies betrifft etwa Systeme zur biometrischen Kategorisierung oder zur Emotionserkennung. Vor allem gilt dies für Systeme, die durch Stellen des Landes in den Bereichen öffentliche Sicherheit und Schulen eingesetzt werden, weil diese Stellen einer Überwachung durch Bundesbehörden aufgrund der verfassungsrechtlichen Ordnung entzogen sind.

Aber auch für die Verwendung von KI im nicht-öffentlichen Bereich spricht sehr viel dafür, die Marktüberwachung von KI bei den Daten-

schutzaufsichtsbehörden zu verankern, wenn die KI zur Verarbeitung personenbezogener Daten eingesetzt wird. So können widersprüchliche Entscheidungen von Markt- und Datenschutzaufsicht vermieden werden. Zuletzt deuteten politische Pläne hingegen auf eine zentrale Marktaufsicht durch die Bundesnetzagentur hin, die bisher über keine vergleichbaren Erfahrungen in Bereichen des Grundrechtschutzes und der Datenverarbeitung verfügt.

Unabhängig davon, ob der LDI NRW Marktüberwachungsaufgaben zugewiesen werden, wird es aber in jedem Fall eine Zusammenarbeit mit der benannten Marktüberwachungsbehörde geben – durch die in der KI-VO festgelegte Verpflichtung, die Datenschutzaufsichten der Länder an Verfahren der Marktaufsicht zu beteiligen. Eine solche planmäßige Einbeziehung der Datenschutzaufsicht in die Überwachung ist allerdings nach der DS-GVO bisher nicht vorgesehen, so dass sich durch die Kooperationsverpflichtungen nach der KI-VO eine ganz neue Prüftiefe bei allen der Datenschutzaufsicht der Länder unterliegenden Hochrisiko-Verfahren nach KI-VO ergeben wird.

Fazit

Die schon vor dem Inkrafttreten der KI-VO bestehenden datenschutzrechtlichen Fragestellungen wurden durch die KI-VO nicht gelöst. Da die KI-VO den Anwendungsbereich der DS-GVO unberührt lässt und insbesondere keine Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in den verschiedenen Lebenszyklen eines KI-Systems geschaffen wurden, bleibt viel Rechtsunsicherheit. Eine Wahrnehmung der Marktaufischt durch die bestehenden Datenschutzaufsichtsbehörden wäre für eine harmonisierte Anwendung von KI-VO und DS-GVO sinnvoll.

5.3. Generative Künstliche Intelligenz: Was gilt für die Betroffenenrechte?

Der zunehmende Einsatz von generativer KI stellt den Datenschutz vor Herausforderungen. Dürfen personenbezogene Daten zum Training von KI genutzt werden? Was ist mit den in der DS-GVO garantierten Rechten von Betroffenen, Auskunft über die Nutzung ihrer Daten zu erhalten oder Berichtigung zu verlangen? Auch die mittlerweile in Kraft getretene KI-Verordnung löst dieses Spannungsverhältnis nicht auf.

Generative KI ist derzeit in aller Munde. Dahinterstecken – vereinfacht gesagt – Techniken, die mit einer Vielzahl von Informationen angelernt werden, um daraus neue Inhalte herstellen zu können. So kann eine KI beispielsweise darauf trainiert werden, Bilder aus textuellen Beschreibungen zu generieren oder einen Aufsatz zu einem bestimmten Thema zu verfassen. Large Language Models (LLM) bilden die Grundlage für bekannte Anwendungen generativer KI wie ChatGPT, Google Gemini oder Microsoft Copilot. Sie zeichnen sich dadurch aus, dass sie aufgrund ihrer Größe in der Lage sind, menschliche Sprache zu verstehen und zu kreieren. Für das Training dieser Modelle sind dementsprechend sehr große Mengen an Daten erforderlich.

Trainingsdaten aber werden in der Regel auch aus persönlichen Informationen von Menschen gewonnen – und damit kommt der Datenschutz ins Spiel. Bei der Entwicklung und dem Einsatz von generativer KI, und ganz besonders von LLM, ergeben sich aus Trainingsanforderungen und Funktionsweise datenschutzrechtliche Herausforderungen, wenn personenbezogene Daten verarbeitet werden. Dazu gehören vor allem die Fragen nach der Rechtmäßigkeit der jeweiligen Verarbeitung und nach der Umsetzung von Betroffenenrechten. Die LDI NRW hat sich 2024 auch mit diesen Themen intensiv beschäftigt.

Die derzeit wohl effektivsten Verfahren zur Datensammlung in einer für das Training von LLM geeigneten Größenordnung sind das sog. Scraping und Crawling. Dabei werden automatisiert Informationen aus dem Internet extrahiert und für das Training aufbereitet. Die Daten werden nicht genutzt, um sie eins zu eins zu reproduzieren, wie dies etwas bei Suchmaschinen der Fall ist. Vielmehr soll damit trainiert werden, wie Sprache gebildet wird. Dazu werden die Trainingsdaten – vereinfacht beschrieben – in einen sehr kleinteiligen Buchstabensalat zerlegt. Zusätzlich wird darauf geachtet, in welcher Häufigkeit sich die Bestandteile zueinander anordnen. Stellt man an die KI eine Anfrage, schreibt sie einen Text, der auf Basis der Trainingsdaten wahrscheinlich zu der Anfrage passt. Fordert man beispielsweise einen Text über den Wald in Deutschland an, wird man einen Inhalt mit einem sprachlich logischen Satzbau erhalten.

Die KI bildet dazu die wahrscheinlichste Kombination aus dem Buchstabensalat, die auf den Text der Anfrage folgt. Dass der Text inhaltlich richtig ist, ist in der Regel nicht das Ziel eines allgemeinen LLM. Hätten die Trainingsdaten beispielsweise sehr viele Texte enthalten, die sich mit einem Vergleich von Regenwald und Waldvegetation in Deutschland befassen, könnte es durchaus sein, dass der ausgegebene Text etwas zur Ausbreitung von Lianen im deutschen Wald enthält. Die Modelle geben keine gesichert inhaltlich richtigen Ergebnisse aus, sondern nur linguistisch sehr wahrscheinliche aufeinander folgende Wörter und Sätze. Neuere Systeme versuchen diese Problematik zu lösen, indem sie auf eine zusätzliche Wissensbasis zugreifen, die in die Generierung der Antworten einfließt (sog. Retrieval-Augmented-Generation). Die Wissensbasis basiert im Gegensatz zum Modell nicht auf Wahrscheinlichkeiten, sondern auf Fakten.

So kompliziert diese Systeme aber sind, so schwierig wird deren datenschutzrechtliche Einordnung. Hier stehen vor allem Fragen nach der Rechtsgrundlage für eine Verarbeitung personenbezogener Daten und die Durchsetzung von Betroffenenrechten im Raum.

Bei der Bewertung der Rechtmäßigkeit dieser Datenverarbeitung ist zwischen der Entwicklungsphase und der Nutzungsphase generativer KI zu unterscheiden. Die Entwicklungsphase kann wiederum in zwei Abschnitte aufgeteilt werden. Der erste Abschnitt umfasst die Zusammenstellung und die Vor- und Aufbereitung von Trainingsdaten. Der zweite Abschnitt ist die eigentliche Trainingsphase, wenn das KI-Modell mit diesen Daten trainiert wird, also der erstellte Trainingsdatensatz in das KI-Modell eingespeist und das Modell damit erstellt wird. Die Bewertung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist für die Phasen und Abschnitte separat vorzunehmen.

Zu berücksichtigen ist, dass Trainingsdaten insbesondere von LLM regelmäßig in großem Umfang personenbezogene Daten enthalten und oft auch besondere Kategorien personenbezogener Daten. In der Praxis wird die Verarbeitung meist auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f der DS-GVO als Rechtsgrundlage gestützt. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Wie der Europäische EDSA in seinen Leitlinien 01/2024 festgelegt hat, kann ein Interesse als berechtigt angesehen werden, wenn die folgenden drei Kriterien erfüllt sind:

1. Das Interesse ist rechtmäßig,

2. das Interesse ist klar und präzise formuliert, und

3. das Interesse ist real und gegenwärtig und nicht spekulativ.

Die Datenverarbeitung muss zudem zur Zweckerreichung erforderlich sein. Das bedeutet, dass die Verarbeitung das mildeste Mittel für die Wahrung des Interesses ist. Außerdem darf es keine andere Maßnahme geben, mit der das Interesse genauso effektiv, aber mit geringerer Eingriffsintensität erfüllt würde.

Bei der Entwicklung von LLM sind andere Mittel als das Scraping und Crawling des Internets zumeist nicht gleich effektiv, um gute Entwicklungsergebnisse zu erzielen. Fraglich ist allerdings, ob das Interesse des Verantwortlichen nicht auch durch die Verarbeitung von anonymisierten Daten erreicht werden könnte. Dies wird etwa bei KI-Sprachmodellen, deren Zweck auch die Ausgabe von personenbezogenen Daten ist, in der Regel nicht der Fall sein. Allerdings werden allenfalls Beispiele für personenbezogene Daten benötigt, um zu lernen, wie Sprache funktioniert. Es ist nicht notwendig, dass ein KI-Modell den Namen und die E-Mail-Adresse einer bestimmten Person kennt. Bei der Beurteilung der Erforderlichkeit der Datenverarbeitung ist deshalb auch zu prüfen, wie viele personenbezogene Daten verarbeitet werden und ob dies zur Verfolgung des berechtigten Interesses verhältnismäßig ist. Dies gilt auch mit Blick auf den im Datenschutzrecht verankerten Grundsatz der Datenminimierung, also die Pflicht, stets möglichst wenig personenbezogene Daten einzusetzen.

Im Rahmen der zusätzlich notwendigen Interessenabwägung sind zudem die Interessen des Verantwortlichen den Interessen, Grundrechten und Grundfreiheiten der von der Verarbeitung Betroffenen gegenüberzustellen. Bedeutsam sind dabei unter anderem die Aussagekraft und die Auswirkung der verarbeiteten Daten, die Pflicht zur Datenminimierung sowie die technischen und organisatorischen Maßnahmen zur Minderung des Risikos für die betroffenen Personen. Außerdem muss berücksichtigt werden, wie wahrscheinlich die Identifikation der betroffenen Personen ist und welche Folgen durch die Verarbeitung eintreten können.

In der juristischen Fachliteratur wird zum Teil vertreten, dass bei bereits veröffentlichten Daten das Interesse der Betroffenen daran, dass sie nicht für KI genutzt werden, wenig gewichtig ist. Dies wird mit Art. 9 Abs. 2 Buchstabe e DS-GVO begründet, der das Verbot der Verarbeitung besonderer Kategorien von Daten durchbricht, wenn die betroffene Person diese Daten selbst veröffentlicht hat. Die LDI NRW findet diesen Ansatz dagegen nicht überzeugend. So ist nicht immer klar, dass die Daten von den Betroffenen selbst veröffentlicht worden sind. Aber auch das wäre nicht ohne Weiteres ein Beleg dafür, dass die Interessen der jeweiligen

Betroffenen zurückstehen müssen. Da die Veröffentlichung in der Regel für einen bestimmten Zweck erfolgt und gerade nicht vorhersehbar ist, dass die Daten für das Training eines KI-Modells verwendet werden, muss die Interessenlage in jedem Fall sorgfältig abgewogen werden.

Hier ist auch Erwägungsgrund 47 zur DS-GVO relevant. Danach ist in die Interessenabwägung miteinzubeziehen, ob die betroffene Person zum Zeitpunkt der Verarbeitung vernünftigerweise absehen kann, dass ihre Daten zu einem bestimmten Zweck verarbeitet werden. Ist das nicht der Fall, können die Interessen der betroffenen Person überwiegen. Ob eine vorherige Information daran etwas ändert, ist fraglich. Sie stellt jedenfalls keine Begründung für die Rechtfertigung einer Datenverarbeitung dar.

Zu betrachten sind schließlich die Risiken und Schäden, die durch generative KI-Modelle verursacht werden können. Betroffene Personen, deren Daten für die Entwicklung generativer KI verarbeitet werden, können Schäden entweder im Zusammenhang mit der Erhebung und Verarbeitung der Trainingsdaten oder wegen der Verwendung des generativen KI-Modells erleiden. Sie können die Kontrolle über ihre personenbezogenen Daten verlieren, da sie nicht über deren Verarbeitung informiert werden und daher nicht in der Lage sind, ihre Betroffenenrechte auszuüben oder die Auswirkungen dieser Verarbeitung auf sie zu bewerten. Zudem können generative KI-Modelle etwa dazu verwendet werden, falsche Informationen über betroffene Personen zu generieren, die zu negativen Konsequenzen für diese führen. Weiterhin ist die Fähigkeit des Systems zu berücksichtigen, Schlussfolgerungen zu ziehen (Inferenzmächtigkeit). Es ist noch nicht abzusehen, welche Risiken dadurch für Menschen entstehen, deren Daten im Trainingsdatensatz enthalten sind. Es fehlen bisher Erkenntnisse darüber, welche Schlussfolgerungen über nicht-veröffentlichte Informationen durch das Training des Systems möglich sind und welche Fähigkeiten das System durch die zur Verfügung gestellten Trainingsdaten erlangt. Dies ist unabhängig von der Frage zu betrachten, ob und wie diese Fähigkeiten eventuell im weiteren Verlauf wieder neutralisiert werden können.

Im Ergebnis ist deshalb in jedem Einzelfall gründlich zu prüfen und zu dokumentieren, ob die Voraussetzungen von Art. 6 Abs. 1 Buchstabe f DS-GVO erfüllt sind. Werden besondere Kategorien personenbezogener Daten verarbeitet, sind zusätzlich die Anforderungen von Art. 9 DS-GVO zu beachten.

Neben der Prüfung, ob die Verarbeitung personenbezogener Daten für Training oder Betrieb eines KI-Modells auf eine Rechtsgrundlage gestützt werden kann, stellt sich zudem die Frage, wie die Betroffenenrechte aus der DS-GVO realisiert werden können. So müssen die Verantwortlichen gewährleisten, dass betroffene Personen ihre Rechte auf Datenberichtigung gemäß Art. 16 DS-GVO und -löschung gemäß Art. 17 DS-GVO ausüben

können. Für beide Rechte müssen organisatorische und technische Verfahren konzipiert werden, damit die Rechte auch wirksam ausgeübt werden können. Dafür sind die Vorgaben der datenschutzkonformen Technikgestaltung umzusetzen.

Beim Einsatz von KI-Systemen kann es aus unterschiedlichen Gründen dazu kommen, dass unrichtige personenbezogene Daten verarbeitet werden. Viele Anbietende von KI-Systemen (insbesondere LLM-Chatbots) weisen sogar ausdrücklich darauf hin, dass Anwendende sich nicht auf die Richtigkeit der Ergebnisse verlassen können, sondern diese überprüfen müssen. Bei personenbezogenen Daten besteht bei Unrichtigkeit jedoch ein Recht der betroffenen Personen auf Berichtigung. Diese Berichtigung muss in einem KI-System umsetzbar sein, zum Beispiel durch Korrektur von Daten oder durch ein Nachtraining („Fine Tuning").

Geht es um die Löschung von Daten, ist zu beachten, dass einige KI-Systeme durch die Verknüpfung unterschiedlicher Daten einen Personenbezug herstellen können. Bei der Löschung personenbezogener Daten muss deshalb sorgfältig darauf geachtet werden, dass eine Wiederherstellung des Personenbezugs dauerhaft unmöglich ist. In der Praxis ist dies aufgrund der technischen Funktionsweise von KI-Systemen und den zugrundeliegenden Modellen jedoch problembehaftet. So können Daten oftmals nur durch ein erneutes Training der Modelle mit bereinigten Trainingsdaten entfernt werden.

Auch die weiteren Betroffenenrechte auf Auskunft über die Verarbeitung, auf Einschränkung der Verarbeitung und auf Datenübertragbarkeit sowie das Widerspruchsrecht müssen bei der Gestaltung der KI-Anwendung berücksichtigt werden. Die Frage, ob ein in den Trainingsdaten enthaltener Name aus dem oben beschriebenen Buchstabensalat wieder rekonstruiert wird und in welchem Sachzusammenhang er dann steht, ist durch die beim Training festgestellten Wahrscheinlichkeiten bestimmt. Daher ist es auch für die Hersteller*innen des Systems kaum zu beantworten, was das System im Einzelnen zu einer bestimmten Person ausgibt.

Die mittlerweile in Kraft getretene KI-VO löst dieses Spannungsverhältnis zwischen KI und den Betroffenenrechten nach der DS-GVO nicht auf. Die KI-VO enthält keine Regelungen zu den Betroffenenrechten oder deren Modifikation, so dass die Problematik hinsichtlich der Umsetzung der Betroffenenrechte nach der DS-GVO weiterhin besteht.

Zwischenzeitlich hat der EDSA eine Stellungnahme zur Verwendung personenbezogener Daten für die Entwicklung und Einführung von KI-Modellen (Opinion 28/2024) verfasst. In dieser Stellungnahme wird untersucht, 1) wann und wie KI-Modelle als anonym angesehen werden können, 2) ob und wie berechtigtes Interesse als Rechtsgrundlage für die Entwicklung oder Nutzung von KI-Modellen verwendet werden kann

und 3) was passiert, wenn ein KI-Modell unter Verwendung unrechtmäßig verarbeiteter personenbezogener Daten entwickelt wird. Die Stellungnahme berücksichtigt auch die Verwendung von Erst- und Drittdaten.

Fazit

Die DS-GVO setzt der Entwicklung und Anwendung von KI enge Grenzen, wenn personenbezogene Daten verarbeitet werden. Mit der KI-VO tritt nur eine zweite europäische Verordnung neben die DS-GVO – das Spannungsverhältnis zwischen der DS-GVO und der Entwicklung und Nutzung von KI wird damit nicht gelöst. Soll das Potenzial von KI genutzt werden, bedarf es wahrscheinlich eines eigenen spezifischen Schutzkonzepts für die Datenschutzrechte der Betroffenen.

5.4. Emotionserkennungssoftware hat im Callcenter nichts zu suchen



Unternehmen nutzen zunehmend Künstliche Intelligenz (KI), um Kund*innengespräche besser einordnen zu können. Dabei kam in einem Fall auch Software zum Einsatz, die Emotionen erkennen und bewerten soll. Die LDI NRW sieht darin eine Verletzung von Persönlichkeitsrechten.

Das dürfte mittlerweile jede*r kennen: Wer telefonisch bei einem Unternehmen anfragt, landet direkt in einem Call-Center, wo Mitarbeiter*innen, die teilweise über die ganz Welt verstreut sitzen, die Fragen beantworten

oder andere Servicedienste verrichten. Neuster Trend in dieser Call-Center-Branche: der Einsatz von KI – und hier speziell die KI-gestützte Emotionsanalyse. Sie soll Muster in der Sprache identifizieren und analysieren, damit sich die Mitarbeiter*innen besser auf ihre Gesprächspartner*innen einstellen können. Aber ist das überhaupt zulässig?

Die LDI NRW hat sich im vergangenen Jahr mit einem Unternehmen im Online-Marketing beschäftigt, das sogar damit warb, eine solche Software einzusetzen. Die Firma bearbeitet als Dienstleisterin für andere Unternehmen unter anderem Beschwerden im telefonischen Kund*innendienst. Hierzu betreibt sie Call-Center mit eigenen Mitarbeitenden, sog. Agent*innen.

Das eingesetzte KI-System analysierte dabei in Echtzeit Sprachmelodie, Intensität, Rhythmus und Klang sowohl der Kund*innen- als auch der Agent*innen-Stimmen. Insgesamt wurden mehr als 6.000 Parameter überprüft, um daran Emotionen wie Wut, Ärger, aber auch Freundlichkeit abzulesen. Die einzelnen Emotionsbestimmungen wurden den Agent*innen während des Gesprächs grafisch als positiv oder negativ dargestellt. Die Agent*innen sollten so die Emotionen der Gesprächspartner*innen berücksichtigen und ihre Beratung adäquat anpassen. Zugleich wurden auch die Stimmen der Agent*innen selbst mit dem System analysiert, um auch deren Verhalten gegenüber ihren Gesprächspartner*innen zu optimieren.

Die LDI NRW hat dieses System auf seine Vereinbarkeit mit dem Datenschutz hin überprüft. Sie ist zu dem Schluss gekommen, dass es sich hier um einen massiven und nicht gerechtfertigten Eingriff in die Persönlichkeitsrechte sowohl der Kund*innen als auch der Agent*innen handelt.

Zunächst einmal ist festzuhalten, dass es sich bei der durchgeführten Analyse der Sprache und der Stimme von Beschäftigten im Callcenter ebenso wie von den dort Anrufenden um eine Datenverarbeitung im Sinne der DS-GVO handelt. Stimme und Sprache von Menschen sind personenbezogene Daten. Die Verarbeitung dieser Daten mit einem KI-Systems erfolgte im konkreten Fall ohne Rechtsgrundlage. Weder lässt sich der Einsatz des Emotionserkennungssystems damit rechtfertigen, dass es notwendig wäre sicherzustellen, dass die Beschäftigten ihren Arbeitsvertrag im Callcenter ordnungsgemäß erfüllen. Noch hätte der Einsatz des Systems auf eine Einwilligung der Beschäftigten gestützt werden können.

Eine Überwachung der Arbeitsleistung anhand emotionaler Merkmale ist ein tiefgreifender Eingriff in die Persönlichkeitsrechte der Beschäftigten. Ein korrektes Verhalten gegenüber den Anrufer*innen ist Teil ihrer Arbeitspflicht. Die geschuldete Arbeitsleistung besteht aber nicht darin, bei der Arbeit eine bestimmte emotionale Stimmung zu haben, dies darf dementsprechend auch nicht überwacht werden. Zudem besteht die

Gefahr, dass die Mitarbeitenden durch die Emotionserkennungssoftware lückenlos während der gesamten Arbeitszeit unter Beobachtung stehen und sie dadurch unter erheblichen psychischen Anpassungsdruck gesetzt werden.

Der Einsatz eines solchen Systems kann auch nicht durch eine Einwilligung der Beschäftigten legitimiert werden. Das ist nur dann denkbar, wenn die Analyse und Anzeige lediglich für die einzelnen Agent*innen verfügbar und aktivierbar gewesen wäre (Opt in). Die Anzeige war aber stets auch für die Teamleiter*innen verfügbar. Diese konnten ihre Mitarbeiter*innen durch die ständige Echtzeitanalyse permanent überwachen.

Die Kund*innen wurden über die Auswertung ihrer Stimmen erst gar nicht unterrichtet. Ein überwiegendes berechtigtes Interesse des Unternehmens an der Verarbeitung von Sprachdaten der Kund*innen, das die Datenerhebung hätte rechtfertigen können, bestand gegenüber dem Recht der Kund*innen auf Schutz ihrer personenbezogenen Daten ebenfalls nicht.

Zudem wurden die möglichen Risiken durch das Unternehmen nicht sorgfältig geprüft. Eine Datenschutzfolgenabschätzung (DSFA) wurde nicht durchgeführt. Eine solche DSFA ist erforderlich, wenn eine Form der Datenverarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt" (Art. 35 Abs. 1 DS-GVO). Emotionserkennungssysteme gehen regelmäßig mit hohen Risiken für die Betroffenen einher. Dementsprechend qualifiziert auch die inzwischen verabschiedete KI-VO der EU derartige Emotionserkennungssysteme als Hochrisiko-KI-Systeme, die besonderen Anforderungen unterliegen.

Eine DSFA muss sich insbesondere mit Abhilfemaßnahmen befassen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. Wäre eine solche Analyse durchgeführt worden, hätte die Verantwortliche das Fehlen der Rechtsgrundlagen feststellen können. Der Einsatz der KI-Emotionsanalyse konnte im Ergebnis sowohl gegenüber den Agent*innen als auch den Kund*innen auf keine Rechtsgrundlage gestützt werden, die den Einsatz gestattet hätte. Die KI-gestützte Datenverarbeitung war daher unzulässig.

Das Unternehmen hat den Einsatz des KI-Systems unmittelbar nach dem Beginn der Prüfung durch die LDI NRW zwar eingestellt. Dies geschah aber vorwiegend aufgrund von negativer Berichterstattung in der Presse. Eine Sanktion des unzulässigen Einsatzes durch die LDI NRW wird geprüft.

Fazit

Die KI-gestützte Auswertung von Stimme zur Emotionserkennung stellt ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen dar, da sie weitgehende Einblicke in die Persönlichkeit zulässt. Der Einsatz einer entsprechenden Software in Call-Centern zur Optimierung der Kund*innenbetreuung ist ein schwerwiegender Eingriff in die Persönlichkeitsrechte von Kund*innen und Mitarbeiter*innen und nicht zulässig.

6. Internet, Medien und Digitales



6.1. Gibt es ein Recht auf ein analoges Leben?

Der Kauf von Fahrkarten, der Kontakt zum Energieversorger oder die Eintrittskarte fürs Konzert – fast alles kann heute online erledigt werden. Was aber, wenn der digitale Weg die einzige Möglichkeit ist, um zentrale Dienstleistungen der Daseinsvorsorge in Anspruch zu nehmen? Was ist dann mit den Menschen, die sich schwertun im Umgang mit digitalen Medien?

Manche Dienstleistung kann man heute nur noch in Anspruch nehmen, wenn man eine App auf dem Handy installiert. Großes Aufsehen erregte die Deutsche Bahn, als sie die Bahn-Card nur noch digital anbieten wollte. Personen, die nicht oder nur eingeschränkt in der Lage sind, die technischen Applikationen zu bedienen oder auch kein Handy besitzen, wären dann von dem Angebot ausgeschlossen. Und die Bahn ist nicht das einzige Unternehmen, das sich Einspareffekte durch solche Digitalisierungsmaßnahmen verspricht.

Die DSK hat zu diesem Problem die Entschließung „Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen!" verabschiedet, die im Anhang zu diesem Bericht abgedruckt ist. Die datenschutzrechtlichen Fragen zu ausschließlich digital angebotenen daseinsvorsorgerelevanten Dienstleistungen wurden zuvor in einer Arbeitsgruppe aufbereitet, an der sich auch die LDI NRW beteiligt hat.

Tatsächlich ist zu beobachten, dass es einen Trend gibt, Bürger*innen in eine rein digitale Welt zu drängen. Die Datenschutzaufsichtsbehörden haben sich daher intensiv mit der Frage befasst, ob das Datenschutzrecht und hier maßgeblich die DS-GVO Ankerpunkte enthält, die einen Anspruch stützen, Dienste auch analog zu nutzen. Hierbei wurden insbesondere Dienstleistungen in den Blick genommen, die jeder

in unserer Gesellschaft benötigt, um am gesellschaftlichen Leben wirtschaftlich, sozial und kulturell teilzuhaben.

Grundsätzlich unterscheidet die DS-GVO nicht zwischen analoger und digitaler Datenverarbeitung. Vielmehr ist sie technikneutral formuliert und steht insofern zukünftigen technischen Entwicklungen nicht entgegen. Entscheidend ist, dass auch die digitale Datenverarbeitung nur dann zulässig ist, wenn sie mit den in Art. 5 Abs. 1 DS-GVO normierten datenschutzrechtlichen Grundsätzen in Einklang steht und die in Art. 6 DS-GVO aufgeführten Voraussetzungen für die Rechtmäßigkeit der Datenverarbeitung erfüllt sind.

Datenverarbeitungen zur Erbringung entsprechender Dienstleistungsangebote müssen insbesondere den Anforderungen an die Rechtmäßigkeit, Zweckbindung und Datenminimierung gerecht werden. Gemeint ist unter anderem, dass es für die konkrete Datenverarbeitung eine Rechtsgrundlage geben und die Verarbeitung auf das für ihren Zweck notwendige Maß beschränkt sein muss. So kann etwa problematisch sein, ob das Unternehmen, das die Daten digital erhebt und sich dafür auf den Vertrag mit seinen Kund*innen beruft, die Datenverarbeitung auf das für den Vertrag Nötige reduziert hat. Weitere Einzelheiten zu den datenschutzrechtlichen Fragen enthält im Übrigen die im Anhang abgedruckte DSK-Entschließung.

Letztendlich wird allerdings die gesellschaftspolitische Frage, in welchem Umfang notwendige Dienstleistungen ausschließlich digital angeboten werden dürfen, nicht durch das Datenschutzrecht geklärt werden. Hier bedarf es gesetzlicher Regelungen, um die Teilhabe an Daseinsvorsorgeleistungen auch solchen Personen zu ermöglichen, denen Fähigkeit oder Willen zur Nutzung von digitalen Endgeräten fehlen. Der Gesetzgeber muss das Interesse an allgemeiner Teilhabe an der Daseinsvorsorge gegen die unternehmerische Freiheit zu ausschließlich digitalen Angeboten abwägen. Um auf das Beispiel der Bahn zurückzukommen: Hier sind Menschen, die öffentliche Verkehrsmittel nutzen, sehr weitgehend auf die Dienstleistungen dieses Unternehmens angewiesen. Für manche Bahnnutzer*innen wäre es ein großes Problem, wenn sie die Dienstleistung nur noch digital bekommen könnten. Die Bahn hat hier wohl inzwischen auch eingelenkt. Aber beispielsweise auch Unternehmen der Energieversorgung drängen ihre Kund*innen in die digitale Kommunikation, obwohl nicht alle Kund*innen diesen Weg mitgehen und ohne fremde Hilfe dann nicht mehr ihre vertraglichen Angelegenheiten regeln könnten. Dies gilt es auch politisch zu begleiten.

Fazit

Eine Diskriminierung von Personen, die kein Internet nutzen können oder wollen oder kein Smartphone besitzen, darf vor allem im Bereich daseinsrelevanter Leistungen nicht erfolgen. Der Datenschutz ist jedoch nicht das geeignete Instrument, die gleichmäßige Teilhabe aller Bürger*innen an diesen Leistungen durchzusetzen. Dazu bedarf es eindeutiger gesetzlicher Regelungen.

6.2. Datenschützer*innen stellen strengere Regeln für Website-Betreiber*innen auf

Für Unternehmen, die Tracking-Techniken einsetzen, wird der rechtliche Gürtel enger geschnallt. Nachdem die europäischen Aufsichtsbehörden strengere Leitlinien aufgestellt haben, sind nun auch die deutschen Datenschutzaufsichten nachgezogen – insbesondere mit Blick auf eine nötige Einwilligung von Website-Nutzer*innen.

Die DS-GVO ist nur eine der Rechtsordnungen, die Website-Betreiber*innen regelmäßig beachten müssen: daneben gilt für sie auch noch eine EU-Richtlinie, die sog. ePrivacy-Richtlinie, sowie deren Umsetzung in deutsches Recht. Die wiederum trägt den sperrigen Namen „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten", abgekürzt TDDDG. Alle diese Vorschriften müssen Unternehmen beachten, die ihre Kund*innen „tracken", also nähere Informationen über die Besucher*innen ihrer Website erhalten wollen.

Eine besonders wichtige Rolle spielt dabei § 25 des TDDDG, der Art. 5 Abs. 3 der ePrivacy-Richtlinie umsetzt. Die Vorschrift dient dem Schutz der Privatsphäre der Nutzer*innen, indem sie die Integrität von Endgeräten schützt. Nur mit einer informierten Einwilligung der Nutzer*innen dürfen Informationen auf deren Endgeräten gespeichert oder darf auf bereits gespeicherte Informationen zugegriffen werden. Unter einer informierten Einwilligung versteht man, dass die betroffene Person ausreichend über Umfang und Reichweite der Verarbeitung ihrer Daten informiert wurde. Sie soll sich darüber im Klaren sein, worin genau sie einwilligt.

Dies Vorschrift des § 25 TDDDG kommt insbesondere dann zur Anwendung, wenn Website-Betreiber*innen sog. Cookies setzen, die dazu dienen, Seitenbesucher*innen wiederzuerkennen und nähere Informa-

tionen über deren Internetnutzung zu erhalten. Da jedoch immer mehr Seitenbesucher*innen Cookieblocker und andere Instrumente einsetzen, um Cookies zu verhindern, sind viele Website-Betreiber*innen mittlerweile dazu übergegangen, andere Trackingtechniken wie URL-Tracking und IP-Tracking zu nutzen. Während beim Einsatz von Cookies kleine Dateien im Browser der Internetnutzer*innen abgelegt und ausgelesen werden, ist bei diesen neueren Techniken häufig weniger klar, ob tatsächlich ein Zugriff auf das Endgerät vorliegt.

Das hat in der Folge in Europa zu Unsicherheiten über die Reichweite des Anwendungsbereichs des Art. 5 Abs. 3 ePrivacy-Richtlinie und der zugehörigen nationalen Vorschriften geführt – woraufhin verschiedene europäische Aufsichtsbehörden, darunter auch die deutschen Datenschutzaufsichtsbehörden, in Orientierungshilfen ihr jeweiliges Verständnis dazu kommuniziert haben.

Diese Entwicklung ist nun noch einen Schritt weiter gegangen. Nachdem der EDSA in eigenen Leitlinien ein europaweit einheitliches Verständnis zur Reichweite der Vorschriften festgelegt hat, sind die deutschen Datenschutzaufsichten geschlossen nachgezogen. Sie haben das Verständnis des EDSA in ihrer aktuellen Orientierungshilfe Digitale Dienste der DSK berücksichtigt, die im November 2024 beschlossen wurde.

Die DSK hat damit ihre Auffassung geändert und sich dem weitergehenden Verständnis des EDSA zu Art. 5 Abs. 3 ePrivacy-Richtlinie angeschlossen. Im „allgemeinen Teil" der EDSA-Leitlinie sind die Begrifflichkeiten noch weitestgehend mit denen der alten Orientierungshilfe Digitale Dienste der DSK aus 2021 in Einklang zu bringen. Bei den ebenfalls in der Leitlinie aufgelisteten Anwendungsfällen zeigt sich hingegen ein anderes Bild. So unterfallen nun auch neue Trackingtechniken wie URL-Tracking und IP-Tracking dem Anwendungsbereich des Art. 5 Abs. 3 ePrivacy-Richtlinie mit der Folge, dass für deren rechtmäßigen Einsatz in der Regel Einwilligungen von betroffenen Nutzer*innen bzw. Teilnehmer*innen einzuholen sind. Das war nach dem bisherigen Verständnis der deutschen Datenschutzaufsichtsbehörden nicht der Fall.

Die erweiterte Anwendung von Art. 5 Abs. 3 der ePrivacy-Richtlinie hat zudem weitreichende Auswirkungen für solche Verantwortliche, die europaweit tätig sind. Denn werden die neuen Tracking-Techniken in verschiedenen Mitgliedstaaten eingesetzt, kann grundsätzlich jede Aufsichtsbehörde, die in einem Mitgliedstaat zuständig ist, für den dortigen Einsatz eine entsprechende Prüfung vornehmen. Eine federführende Behörde gibt es – anders als im Rahmen der DS-GVO – nicht. Auf die weitere Verarbeitung der ausgelesenen Daten ist allerdings – sofern es sich um personenbezogene Daten handelt – weiterhin die DS-GVO anwendbar.

Fazit

Verantwortliche, die Tracking-Techniken einsetzen, sollten noch einmal sorgfältig prüfen, ob die Voraussetzungen eines rechtmäßigen Einsatzes vorliegen. Dies gilt insbesondere, soweit sie bislang davon ausgegangen sind, dass die von ihnen genutzten Techniken nicht unter Art. 5 Abs. 3 ePrivacy-RL bzw. § 25 TDDDG fallen. Andernfalls sollten sie Einwilligungen von betroffenen Nutzer*innen einholen.

7. Schule und Bildung



7.1. Gute Nachricht bei der Digitalisierung der Schule – Forschungsprojekt DIRECTIONS kommt voran

Schulen und Schulträger sind häufig mit der Frage überfordert, welche digitalen Anwendungen sie ohne datenschutzrechtliche Bedenken einsetzen können. Hier setzt das Forschungsprojekt DIRECTIONS an, das sich mit einer Zertifizierung von Datenverarbeitungsvorgängen bei Informationssystemen im Bildungssektor beschäftigt – und dabei von der LDI NRW als zuständige Genehmigungsbehörde begleitet wird.

Ob iPad, Smartphone oder Computer – in der Schule der Zukunft wird vor allem digital gelernt. Doch was Bildungspolitiker*innen schon länger propagieren, hinterlässt in der Praxis noch immer viele Fragezeichen – auch in Sachen Datenschutz. Oft fällt es Schulen und Schulträgern schwer, in der Masse der möglichen digitalen Anwendungen die für sie passenden und datenschutzkonformen Lösungen zu finden.

Hier setzt das vom Bundesministerium für Forschung und Bildung geförderte Projekt DIRECTIONS (Data Protection Certification for Educational Information Systems) an. Es soll Schulen und Schulträgern helfen, durch die Zertifizierung von Datenverarbeitungsvorgängen schulspezifische Anwendungen zu finden, die datenschutzkonform eingesetzt werden können. Die LDI NRW erhofft sich dadurch eine Verbesserung des Datenschutzes im Schulbereich und wird in ihrer Funktion als Genehmigungsbehörde das dafür erforderliche Verfahren zur Genehmigung von Zertifizierungskriterien eng begleiten. Dasselbe gilt für die sich daran anschließenden Verfahren zur Akkreditierung von Zertifizierungsstellen im Rahmen ihrer Zuständigkeit.

Sowohl auf dem Jahrestreffen der behördlichen Datenschutzbeauftragten an Schulen in NRW als auch bei einem Informationstreffen mit den Projektteilnehmer*innen hatte die LDI NRW Gelegenheit, sich über den aktuellen Stand des Projekts zu informieren. Zwischenzeitlich hat das Projektteam eine aktualisierte Version des Kriterienkatalogs für die zukünftige DIRECTIONS-Zertifizierung nach Art. 42 der DS-GVO veröffentlicht, abrufbar unter https://publikationen.bibliothek.kit.edu/1000172025. Dort werden die datenschutzrechtlichen Anforderungen an bestimmte Verarbeitungsvorgänge (etwa bei der Nutzung von Videokonferenzsystemen) beschrieben und auch die landesspezifischen Besonderheiten im Schuldatenschutzrecht abgebildet.

Das Projektteam sammelt nun Feedback zu dem Kriterienkatalog, um erforderliche Änderungen oder Anpassungen vorzunehmen. Dies soll die Basis für einen Antrag auf Programmprüfung und Genehmigung der Zertifizierungskriterien bilden.

Fazit

Noch gibt es keine schulspezifischen Zertifizierungen. Die LDI NRW ist aber startklar und wird ihren Beitrag dazu leisten, dass die dafür notwendigen Verfahren auf den Weg gebracht werden.

7.2. iPads im Unterricht: Landesdatenschutzbeauftragte gibt Hinweise zur datenschutzgerechten Nutzung

Sind die Tablets von Apple sicher, soweit es um die Daten von Schüler*innen und Lehrkräften geht? Schulen stehen hier vor großen Herausforderungen, ihre Pflichten zum Schutz dieser Daten zu erfüllen. Denn Vertragsunterlagen und Datenschutzrichtlinie des US-Konzerns legen nahe, dass auf dem iPad erfasste Nutzungsdaten auch in die USA übermittelt werden.

Die Digitalisierung des Unterrichts schreitet voran. Spätestens seit Corona gehören iPads des US-Konzerns Apple an vielen Schulen zum Standard-Arbeitsmittel. Doch noch sind einige Rechtsthemen ungeklärt, Schulträger, Lehrer*innen und Eltern haben Fragen beim Umgang mit den Geräten. Die LDI NRW hat deshalb im vergangenen Jahr daran gearbeitet, Antworten auf die gängigsten Fragen zu finden. Als Grundlage diente dabei neben dem Schulgesetz NRW (SchulG) die DS-GVO.

- **Welche Vorgaben müssen Schulen beim Einsatz von iPads einhalten?**

Schulen dürfen für den Einsatz digitaler Lehr- und Lernmittel die Daten der Schüler*innen, Eltern und Lehrkräfte verarbeiten, soweit dies für ihre Aufgabenerfüllung erforderlich ist (§ 120 Abs. 5 Satz 1 und § 121 Abs. 1 Satz 1 SchulG). Die Systeme müssen zum einen selbst den datenschutzrechtlichen Anforderungen genügen (Art. 5, 24, 25, 32, 44 ff. DS-GVO). Zum anderen ist ihr Einsatz nur insoweit zulässig, wie die Verarbeitung der hierfür erforderlichen Daten durch die Schule erfolgt, das heißt in ihrem Verantwortungsbereich. Hierzu muss sie die Daten selbst verarbeiten oder durch einen Auftragsverarbeiter verarbeiten lassen. Die verantwortlichen Schulen müssen die datenschutzgerechte Datenverarbeitung bei einer Überprüfung im Einzelfall im Rahmen ihrer Rechenschaftspflicht darlegen können (Art. 5 Abs. 2 DS-GVO).

- **Lassen sich diese Vorgaben beim Einsatz von iPads und bei der Nutzung der iCloud umsetzen?**

Schulen müssen sich damit auseinandersetzen, dass sich aus der **Apple-Datenschutzrichtlinie** und dem **Apple-Business-Manager-Vertrag** Anhaltspunkte dafür ergeben, dass von Apple erfasste Nutzungsdaten auch zur Verbesserung der Produkte und zu weiteren internen Zwecken des Unternehmens in die USA übermittelt werden. Denn dort findet die primäre Produktentwicklung statt. Apple gehört aktuell nicht zu den Unternehmen, die erklärt haben, dass sie an dem Trans-Atlantic Data Privacy Framework teilnehmen, so dass der entsprechende EU-Angemessenheitsbeschluss für Übermittlungen personenbezogener Daten in die USA für Apple nicht gilt. Darüber hinaus gibt es auch Hinweise auf eine Datenübermittlung in weitere Drittländer ohne angemessenes Datenschutzniveau.

- **Wie können Schulen einen möglichst datenschutzgerechten Einsatz von iPads sicherstellen?**

Teils können rechtlich ungeklärte Datenübermittlungen technisch unterbunden werden. Dabei bewertet die LDI NRW den Verzicht auf die Nutzung der iCloud-Funktionalitäten als ein probates Mittel, um den datenschutzgerechten Einsatz dieser Produkte zu ermöglichen. Der Verzicht ist grundsätzlich geeignet, mögliche unzulässige Datenübermittlungen einzuschränken und die Verarbeitung der Daten von Schüler*innen und Lehrkräften auf die EU bzw. den europäischen Wirtschaftsraum zu begrenzen. Im Übrigen stellt die Nutzung schulischer iPads im Vergleich zur Nutzung privater iPads die datenschutzfreundlichere Alternative dar. Bei der Nutzung eines

privaten Geräts zu schulischen Zwecken sowie bei der Einrichtung eines privaten Apple-Accounts auf einem schulischen Gerät besteht das Risiko, dass Apple Daten zur schulischen Nutzung des iPads mit Daten zur privaten Nutzung verknüpfen kann. Dies kann am wirksamsten verhindert werden, wenn für schulische Zwecke ausschließlich ein schulisches iPad ohne personalisierten Apple-Account genutzt wird.

■ Können die Daten der Schüler*innen per Backup in der iCloud gesichert werden?

Der LDI NRW ist aus der Beratungspraxis bekannt, dass die Schulträger großes Interesse daran haben, „managed Apple-Accounts" einzusetzen, um die Daten der Schüler*innen in der iCloud zu verwalten. Hierdurch lasse sich sicherstellen, dass wichtige Daten der Nutzer*innen wie Vorbereitungsmaterialien der Schüler*innen für die Abiturprüfungen nicht verloren gingen. iPads seien anerkannte Lehrmittel und ihr Einsatz auch in Prüfungen erforderlich. Daher sei es wichtig, dass ein iPad im Bedarfsfall kurzfristig ersetzt werden könne.

Beim Einsatz von „managed Apple-Accounts" werden allerdings personenbezogene Inhaltsdaten in der iCloud verarbeitet. Diese Daten müssen wiederum vor unbefugten Übermittlungen in Drittländer und vor unberechtigten Zugriffen – etwa durch Weitergabe an Behörden in den Drittstaaten – gesichert werden. Auch wenn die Daten in diesen Backups auf verschiedenen Servern gespeichert werden, stellt sich also die Frage, wie stark die Daten gegen Apple selbst und gegen staatliche Zugriffe geschützt sind.

Aus Sicht der LDI NRW ist bei der Nutzung der iCloud insbesondere Folgendes zu beachten:

Apple gehört aktuell nicht zu den Unternehmen, die erklärt haben, dass sie an dem Trans-Atlantic Data Privacy Framework teilnehmen, so dass der entsprechende EU-Angemessenheitsbeschluss für Übermittlungen personenbezogener Daten in die USA für Apple nicht gilt.

Da eine Identifizierung von Schüler*innen und Lehrenden auch über Inhaltsdaten möglich ist und die Nutzung von solchen Daten für eigene Zwecke von Apple vertraglich nicht sicher ausgeschlossen ist, setzt eine datenschutzgerechte Nutzung der iCloud im Schulbereich zum einen voraus, dass pseudonyme Apple-Accounts verwendet und zum anderen die Inhaltsdaten verschlüsselt werden, ohne dass Apple über den Schlüssel verfügt.

Eine Pseudonymisierung im datenschutzrechtlichen Sinne muss gewährleisten, dass die pseudonymisierten Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr den betroffenen Personen zugeordnet werden können. Insbesondere dürfen die mit einem Pseudonym verknüpften Inhaltsdaten keinen Personenbezug aufweisen. Die Nutzung von Namensbestandteilen in Pseudonymen ist regelmäßig ungeeignet. Die zusätzlichen Informationen (beispielsweise Zuordnungstabellen, kryptographische Schlüssel), die die Zuordnung eines Pseudonyms zur betroffenen Person erlauben, müssen gesondert aufbewahrt werden und dürfen nur berechtigten Personen zu legitimen Zwecken zugänglich sein. Beim Einsatz kryptographischer Verfahren zur Pseudonymisierung sind die einschlägigen BSI- oder ENISA-Richtlinien zu beachten.

Um zu verhindern, dass ein Personenbezug über die Inhaltsdaten hergestellt werden kann, empfehlen wir, die in der iCloud gespeicherten Daten zusätzlich zu verschlüsseln. Dabei ist entscheidend, dass die Nutzer*innen eigene Schlüssel für ihre Backups verwenden, ohne dass Apple über diese Schlüssel verfügt. Da dies aktuell nicht möglich ist, regen wir an, dass Schulen und Schulträger hierzu das Gespräch mit Apple suchen. Um zu vermeiden, dass die Schlüssel verloren gehen, könnten sie im Mobile Device Management hinterlegt werden.

- **Welche alternativen Möglichkeiten für ein Backup gibt es?**

Die LDI NRW empfiehlt, datenschutzfreundlichere Lösungen für ein Backup in Betracht zu ziehen. So kann die Nutzung alternativer Clouds in Betracht kommen. Sofern nicht selbst eine Cloud-Lösung bereitgestellt werden soll, ist anzuraten, einen Cloud-Anbieter nach den Kriterien für Souveräne Clouds der DSK auszuwählen. Die Kriterien sind abrufbar unter www.datenschutzkonferenz-online.de/weitere_dokumente.html. Mit diesem ist insbesondere ein Vertrag zur Auftragsverarbeitung abzuschließen.

Weiterhin besteht die Möglichkeit, dass die Nutzer*innen mittels entsprechender Adapter manuell Backups auf USB-Datenträgern vornehmen.

Fazit

Die LDI NRW empfiehlt Schulen und Schulträgern, die iPads einsetzen wollen, auf die Nutzung der iCloud zu verzichten. Sofern sie nicht auf datenschutzfreundlichere Alternativen zur iCloud zurückgreifen wollen, sollten sie – eventuell im Zusammenschluss – versuchen, Apple zu einer datenschutzgerechten Backup-Lösung für Schulen zu motivieren.

7.3. Wenn LeOn in der Schule mithört – Tonaufzeichnungen verlangen eine Einwilligung

Der Einsatz von Aufzeichnungssoftware im Schulunterricht ist aus Datenschutzsicht problematisch. Beim Einsatz solcher Anwendungen, etwa beim Programm LeOn, ist Fingerspitzengefühl wichtig. Die LDI NRW hat sich in einem konstruktiven Austausch mit dem Landesschulministerium dafür eingesetzt, dass LeOn nur bei einer wirksamen Einwilligung von Eltern oder Schüler*innen zum Einsatz kommt.

LeOn heißt in Wirklichkeit „Leseraum Online" und ist kein Schüler, sondern eine webbasierte Anwendung zur Leseförderung für Schüler*innen der zweiten bis sechsten Klasse. LeOn steht den Schulen mit Primarstufe und Sekundarstufe I in NRW seit Beginn des Schuljahres 2023/2024 kostenfrei zur Verfügung. Die Anwendung bietet den Schüler*innen zur Unterstützung ihres Lesetrainings die Möglichkeit, ihre Leseübungen aufzuzeichnen, zu speichern und an die Lehrkraft zu schicken. Das Programm wird über die Bildungsmediathek NRW angeboten, das Schulministerium NRW unterstützt die Schulen im Rahmen seiner Ressortverantwortung bei dessen Einsatz.

Doch LeOn wirft einige datenschutzrechtliche Fragen auf und kann auch Eltern verunsichern. Ist der Einsatz überhaupt zulässig, gibt es dafür bestimmte Voraussetzungen? Die LDI NRW hat 2024 die Beschwerde eines Elternteils gegen diese Tonaufzeichnungen und gegen die Übersendung der Aufzeichnung an die Lehrkraft zum Anlass genommen, die wesentlichen datenschutzrechtlichen Fragestellungen zu beleuchten - und unmittelbar mit dem Ministerium zu klären.

- **Dürfen die Tonaufzeichnungen nur mit Einwilligung der Eltern oder Schüler*innen gemacht werden?**

  Grundsätzlich dürfen Schulen die Daten von Schüler*innen für den Einsatz von Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsystemen verarbeiten, soweit dies für ihre Aufgabenerfüllung erforderlich ist (§ 120 Abs. 5 Satz 2 Schulgesetz NRW – SchulG). Für (dauerhafte) Bild- und Tonaufzeichnungen des Unterrichts benötigen Schulen jedoch die Einwilligung der betroffenen Personen (§ 120 Abs. 6 Satz 1 SchulG).

- **Unter welchen Voraussetzungen sind Einwilligungserklärungen im Zusammenhang mit dem Schulunterricht zulässig?**

  Eine wirksame Einwilligung der Schüler*innen bzw. ihrer Eltern in die Verarbeitung von Bild- und Tonaufzeichnungen des Unterrichts

setzt voraus, dass sie freiwillig erteilt wird und den betroffenen Personen keine Nachteile entstehen, wenn sie nicht einwilligen (§ 120 Abs. 6 Satz 2 und 3 SchulG). Da im Schulbereich ein Ungleichgewicht zwischen den Beteiligten besteht, sind hohe Anforderungen an die Freiwilligkeit der Entscheidung zu stellen. Siehe hierzu auch die Veröffentlichung der LDI NRW „Digitaler Unterricht in Schulen – Der Grundstein ist gelegt", abrufbar unter **www.ldi.nrw.de/digitaler-unterricht-schulen-der-grundstein-ist-gelegt**.

Daher sind Tonaufzeichnungen des Unterrichts, die auf Einwilligungen gestützt werden, nur in eng begrenzten Ausnahmefällen zulässig. Sie kommen beispielsweise dann in Betracht, wenn sie angeboten werden, um die Schüler*innen zu unterstützen oder ihre persönliche Weiterentwicklung zu fördern. Bei solchen Angeboten ist entscheidend, dass die Schüler*innen bzw. ihre Eltern sich nicht dazu verpflichtet fühlen, Tonaufnahmen fertigen zu lassen. Weiterhin kommt es darauf an, dass im Zusammenhang mit den Tonaufnahmen keine Leistungskontrolle oder Notenerfassung vorgesehen ist, sondern die Schüler*innen bzw. ihre Eltern die Hoheit über die Bildaufnahmen haben und selbst darüber entscheiden können, ob, zu welchem Zweck und von wem diese genutzt werden sollen.

■ Werden diese Voraussetzungen bei LeOn erfüllt?

Wenn die Tonaufnahmen, wie bei LeOn vorgesehen, zusätzlich angeboten werden, um die Schüler*innen (ohne Leistungskontrolle oder Notengebung) zu unterstützen und ihre persönliche Entwicklung zu fördern, kommt ein solcher Ausnahmefall in Betracht. Das Schulministerium NRW hat dafür gesorgt, dass die Schüler*innen bzw. ihre Eltern die Tonaufnahmen jederzeit selbst löschen können. Die Eltern werden in der Einwilligungserklärung insbesondere darüber informiert, dass es sich bei LeOn um ein zusätzliches freiwilliges Angebot der Leseförderung handelt und sie jederzeit die Aufnahmen löschen sowie ihre Einwilligungserklärung gegenüber der Schule widerrufen können.

Fazit

Tonaufzeichnungen des Schulunterrichts bedürfen der Einwilligung der Schüler*innen bzw. ihrer Eltern. Eine umfassende und verständliche Information über die Umstände der für Schulen angebotenen Datenverarbeitungen und über die damit verbundenen Betroffenenrechte stärkt das Vertrauen der Eltern und gibt verantwortlichen Schulen Sicherheit im Umgang mit neuen Datenverarbeitungsmethoden.

8. Verwaltung, Inneres und Justiz



8.1. Geplantes Sicherheitspaket der Landesregierung – Bitte keine Schnellschüsse!

Als Reaktion auf den Anschlag in Solingen mit mehreren Toten hat die Landesregierung 2024 ein umfassendes Sicherheitspaket vorgestellt. Dieses enthält etwa Pläne zur Schaffung neuer Überwachungskompetenzen der Sicherheitsbehörden in NRW. Die Umsetzung sollte grundrechtssensibel und ausgewogen bleiben.

Auch im vergangenen Jahr kam es wieder zu mehreren tödlichen Anschlägen in Deutschland. In NRW traf es Besucher*innen eines Stadtfestes in Solingen, drei Menschen starben bei dem Messerattentat, weitere wurden teils schwer verletzt. Die Landesregierung hat daraufhin Pläne für ein Sicherheitspaket veröffentlicht, das vor allem erweiterte Überwachungsbefugnisse für Polizei und Verfassungsschutz enthält. Vorgesehen sind unter anderem der Zugriff des Verfassungsschutzes auf private Videoüberwachungssysteme sowie der Einsatz von Gesichtserkennungssoftware im Internet. Außerdem soll Künstliche Intelligenz (KI) als sog. „virtueller Ermittler" die sozialen Medien digital durchstreifen dürfen.

Die LDI NRW hat bereits öffentlich Stellung dazu bezogen und auf die Gefahr von schweren und unverhältnismäßigen Eingriffen in die Persönlichkeitsrechte der Bürger*innen bei einigen der geplanten Maßnahmen hingewiesen.

Insbesondere ein möglicher Zugriff des Verfassungsschutzes auf private Videoüberwachungsanlagen ist Besorgnis erregend. Die Verfassung garantiert, dass Bürger*innen sich grundsätzlich unbeobachtet frei

entfalten können. Von privater Videoüberwachung wie etwa im öffentlichen Nahverkehr oder an Tankstellen sind allerdings täglich Millionen Menschen betroffen, die für ein Tätigwerden von Sicherheitsbehörden keinen Anlass gegeben haben. Wenn diese Menschen künftig hinter jeder privaten Kamera den mitbeobachtenden Verfassungsschutz vermuten müssen, würde das bei vielen vermutlich dazu führen, dass sie ihr Verhalten in der Öffentlichkeit entsprechend anpassen. Vor einem solchen Szenario aber sollen gerade die im Grundgesetz verankerten Freiheitsrechte schützen. Wie konkret die Landesregierung ihre Pläne hierzu ausgestalten will, war zum Redaktionsschluss noch nicht bekannt. Die LDI NRW wird sich in jedem Fall kritisch und grundrechtssensibel mit ihnen auseinandersetzen.

Das gilt auch für den angedachten Einsatz von KI zur Gesichtserkennung. Dabei handelt es sich um eine freiheitseinschränkende Maßnahme, die alle Bürger*innen betreffen würde, von denen Bilder im Internet kursieren – unabhängig davon, ob sie zu der Fahndung Anlass gegeben haben. Bei Gesichtserkennung gibt es zudem keine eindeutige Trefferquote, so dass auch Personen mit hoher Ähnlichkeit zu einer gesuchten Person fälschlicherweise in das Visier der Sicherheitsbehörden geraten können. Die Beeinträchtigung der freien Entfaltung der Persönlichkeit sowie der freien Meinungsäußerung im Internet ist offenkundig, weil zumindest ein Teil der Nutzer*innen nicht mehr so frei im Netz agieren wird wie bisher. Bilder, die von anderen hochgeladen wurden, verstärken dieses Problem noch, da auf diese Weise auch vorsichtige Menschen in den Fokus einer KI zur Gesichtserkennung geraten können.

Beim Einsatz von KI besteht weiter das generelle Problem, dass diese regelmäßig nur mögliche, aber nicht sichere Ergebnisse erzeugt. Informationen werden aus den Trainingsdaten lediglich auf Grundlage von Erfahrungswerten generiert. Spürbar wird das für Einzelne, wenn sie allein aufgrund ihrer Daten in einen Verdacht geraten, der den Erfahrungen der Trainingsdaten entspricht, aber nichts mit der realen Person zu tun hat.

Der Vorstoß der Landesregierung schließlich, die sog. Vorratsdatenspeicherung erneut aufzugreifen und neu regeln zu wollen, ist nicht überraschend. Er fußt auf einem Urteil des Europäischen Gerichtshofs (EuGH) vom vergangenen Jahr (Urteil vom 30. April 2024, Az. C-470/21). Das Gericht hatte darin Wege aufgezeigt, die die anlasslose Speicherung von IP-Adressen zu bloßen Identifizierungszwecken für allgemeine Strafverfolgungszwecke in einem engen, gesetzlich zu beschreibenden Rahmen ermöglichen. Zu berücksichtigen ist hier allerdings, dass eine generelle und anlasslose Speicherung von Verkehrs- und Standortdaten auf Vorrat weiterhin nicht mit den EU-Grundrechten zu vereinbaren ist, sofern sie zu einer umfassenden Aufhellung der Aktivitäten von Personen erfolgt.

Jede Form der Vorratsdatenspeicherung birgt Missbrauchspotential und weckt Begehrlichkeiten für immer weitere Anwendungsszenarien. Die Erfahrung der LDI NRW als Datenschutzaufsichtsbehörde zeigt, dass Datenpools schnell für weitere Zwecke verwendet werden, wenn sie einmal – unter engen Grenzen – eingeführt wurden. Deswegen bleibt es die Aufgabe der Datenschutzbeauftragten in Deutschland, darauf hinzuwirken, dass geplante Gesetze den vom EuGH gesetzten Rahmen nicht überschreiten.

Terrorakte wie in Solingen oder auch in Magdeburg veranlassen die jeweiligen Regierungen mit großer Regelmäßigkeit dazu, Sicherheitsgesetze zu verschärfen. Doch gerade hoch sensible Eingriffe in Freiheitsrechte verlangen eine gründliche Analyse. Denn zur Wahrheit gehört auch, dass solche Taten auch mit strengsten Sicherheitsmaßnahmen nie gänzlich ausgeschlossen werden können. Wenn sich allerdings ein Mangel an Sicherheitsbefugnissen als ein wesentlicher Faktor erweist, kann das durchaus gesetzliche Änderungen begründen. Diese müssen aber in Bezug auf die Freiheiten aller Bürger*innen verhältnismäßig bleiben.

Fazit

Freiheit bedarf einer gewissen Sicherheit, um sich zu entfalten. Sicherheit ohne Freiheit ist allerdings nicht viel wert. Insoweit müssen die Sicherheitsbedürfnisse und die Auswirkungen auf die Freiheitsrechte ausgewogen bleiben. Dies ist eine wichtige Aufgabe der an der Gesetzgebung beteiligten Organe, die in diesem Zusammenhang auf die Beratung der LDI NRW zurückgreifen können.

8.2. Kontrollbefugnis der LDI NRW über die Staatsanwaltschaften – Konflikt besteht weiterhin

Der Fall ist eigentlich eindeutig: Die LDI NRW darf laut Gesetz die Staatsanwaltschaften in NRW kontrollieren, soweit es um die Einhaltung datenschutzrechtlicher Pflichten geht. Doch sowohl die Staatsanwaltschaft Arnsberg, die Generalstaatsanwaltschaften als auch der Justizminister sperren sich dagegen. Die LDI NRW hat drauf nun mit einer Beanstandung wegen Missachtung ihrer Befugnisse reagiert.

Seit 2020 schon versucht die LDI NRW zu kontrollieren, ob die Staatsanwaltschaft Arnsberg ihren Datenschutzpflichten nachkommt – und etwa Informationen über Freisprüche oder Verfahrenseinstellungen zügig an die Polizei weitergibt, damit dort die Daten der einst Beschuldigten gelöscht werden. Für die Betroffenen ist das wichtig, besteht doch ansonsten die Gefahr, etwa bei der nächsten Verkehrskontrolle fälschlicherweise von der Polizei als mutmaßliche*r Straftäter*in wahrgenommen zu werden.

Doch obwohl das Kontrollrecht der LDI NRW über die Staatsanwaltschaften im Land gesetzlich eindeutig geregelt ist, weigert sich die Staatsanwaltschaft in Arnsberg hartnäckig, Einsicht in ihre Akten zu gewähren – und wird dabei mittlerweile sogar von den Generalstaatsanwaltschaften und dem Justizminister als oberste Aufsichtsbehörde gestützt. Die LDI NRW sah sich daher gezwungen, nun einen Schritt weiter zu gehen und gegenüber der Staatsanwaltschaft Arnsberg eine förmliche Beanstandung auszusprechen. Die Haltung der Justiz-Verantwortlichen betrifft unmittelbar die Unabhängigkeit, die der LDI NRW verfassungs- und europarechtlich zugewiesene ist.

Wie schon in früheren Datenschutzberichten erläutert (27. und 28. Bericht unter 6.5), ergibt sich die Kontrollkompetenz der LDI NRW eindeutig aus dem DSG NRW (§ 60 in Verbindung mit § 35 Abs. 1 Nr. 2 DSG NRW). Daran ändert auch – anders als von der Staatsanwaltschaft Arnsberg und auch dem Justizministerium behauptet – die Neueinführung der Vorschrift des § 500 Strafprozessordnung (StPO) nichts. Zwar müssen danach die Staatsanwaltschaften bei ihrer Arbeit ergänzend zu den datenschutzrechtlichen Regelungen der StPO die einschlägigen Regelungen des BDSG für die Verarbeitung von Daten anwenden. Diese Regelung soll sicherstellen, dass alle Staatsanwaltschaften in Deutschland dieselben datenschutzrechtlichen Vorschriften beachten. In der Begründung für diese Neuregelung wird jedoch ausdrücklich klargestellt, dass dies nicht die Frage der Datenschutzkontrolle berührt. Hier soll es bei der Zuständigkeit der jeweiligen Landesdatenschutzaufsichtsbehörden bleiben. Entgegen dieser eindeutigen Begründung zur Gesetzesänderung vertritt die Staatsanwaltschaft Arnsberg dennoch die Auffassung, dass die

Kontrollkompetenz der LDI NRW entfallen sei, weil § 500 StPO keinen Bezug auf die Regelungen zur Datenschutzkontrolle im BDSG nähme. Dass diese Vorschriften nicht in Bezug genommen wurden, ist indessen konsequent und richtig, denn sie regeln die Datenschutzkontrolle des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die gerade nach der Gesetzesbegründung nicht gewollt war. Das ist insofern auch folgerichtig und passt zur Begründung.

Die Auffassung der Staatsanwaltschaft Arnsberg, dass keine Datenschutzbehörde zuständig für die Kontrolle über die Staatsanwaltschaften sei, ist zudem eklatant europarechtswidrig. Denn nach der JI-Richtlinie, die sich unter anderem mit dem Datenschutz in der Justiz befasst, muss eine Datenschutzaufsichtsbehörde mit der Aufsicht über die Staatsanwaltschaften betraut sein. Eine gesetzliche Ausnahme gilt nur dann, wenn es um Behörden geht, die justizielle Tätigkeiten ausüben. Gemeint sind damit aber unabhängige Gerichte, die auch gegenüber den Datenschutzbehörden in ihrer rechtsprechenden Tätigkeit unabhängig bleiben müssen. Deutsche Staatsanwaltschaften hingegen genießen keine richterliche Unabhängigkeit. Das hat auch der Europäische Gerichtshof klargestellt (Urteil vom 27. Mai 2019, Az. C-508/18 und C-82/19 PPU) – und vom Justizminister im Rechtsauschuss des Landtags auch nicht bestritten. Das Justizministerium nimmt in dieser Sache eine nicht nachvollziehbare Haltung ein. Einerseits bestreitet es die grundsätzliche Kontrollbefugnis der LDI NRW nicht, teilt der LDI NRW aber gleichzeitig mit, die Rechtsauffassung der Staatsanwaltschaft Arnsberg zu teilen, die indessen unter Bezug auf § 500 StPO die Kontrollbefugnis der LDI NRW gänzlich bestreitet.

Die LDI NRW ist befugt, sämtliche personenbezogenen Daten einzusehen, die für ihre Aufgabenerfüllung erforderlich sind. Die Durchführung von Kontrollen gehört dabei zu den klar definierten Aufgaben (§ 60 Abs. 2 DSG NRW). Die Entscheidung darüber, was für die Aufgabenerfüllung erforderlich ist, liegt im alleinigen Ermessen der LDI NRW – kontrollierbar ist das nur durch Gerichte, nicht durch die Staatsanwaltschaften. Im Rahmen der Befugnisse darf die LDI NRW auch die Übersendung bzw. Einsichtnahme von Daten verlangen, weshalb die Staatsanwaltschaften verpflichtet sind, dies vorzunehmen bzw. zu gewähren (§ 60 Abs. 3 DSG NRW). Da die Kontrollen zum Schutz der Rechte der Personen erfolgen, um deren personenbezogene Daten es geht, stehen auch deren Datenschutzrechte der Kontrolle regelmäßig nicht entgegen.

Auf Grundlage dieser eindeutigen Rechtslage hat die LDI NRW bei der Staatsanwaltschaft Arnsberg die dortige mangelnde Kooperationsbereitschaft beanstandet. Justizminister Limbach wurde aufgefordert, von seiner Ressortverantwortung Gebrauch zu machen und für ein rechtmäßiges Verhalten der Staatsanwaltschaft Arnsberg zu sorgen. Das ist bisher aber nicht passiert. Nach wie vor gibt es keine klare Aussage aus dem Justizministerium, dass die Staatsanwaltschaften verpflichtet

sind, Kontrollen durch die LDI NRW zuzulassen. Vielmehr stützt das Justizministerium die Haltung der Staatsanwaltschaft Arnsberg und kritisiert die Art und Weise, in der die LDI NRW kontrollieren möchte. Konkret ist das Justizministerium der Auffassung, die LDI NRW fordere mehr Unterlagen, als für ihre Kontrolle benötigt würden und halte den Grundsatz der Datensparsamkeit nicht ein.

Abgesehen davon, dass die LDI NRW der Staatsanwaltschaft Arnsberg signalisiert hatte, für den konkreten Kontrollanlass über Alternativen zu einer Aktenübersendung gesprächsbereit zu sein, mutet es zusätzlich befremdlich an, wenn das Justizministerium sich berechtigt sieht, die unabhängige Kontrolle durch die LDI NRW hinsichtlich Art und Umfang bestimmen zu wollen.

Neben diesen kaum mehr nachvollziehbaren juristischen Auseinandersetzungen über das „Ob" und „Wie" einer Kontrollbefugnis der LDI NRW gibt es noch eine Kontrollpraxis, die auch nicht verschwiegen werden darf. Wenn sich Einzelpersonen mit Beschwerden an die LDI NRW wenden und die Staatsanwaltschaften von der LDI NRW zur Überprüfung der Beschwerde um Stellungnahme gebeten werden, nehmen alle Staatsanwaltschaften in NRW, einschließlich der Staatsanwaltschaft in Arnsberg Stellung. Demnach scheint sich die abwehrende Haltung in Bezug auf die Kontrollbefugnis der LDI NRW vorrangig auf solche Kontrollen zu beziehen, die die LDI NRW eigenständig initiiert, um die regelmäßige Einhaltung des Datenschutzes zu überprüfen. Eine derartige Beschränkung der Kontrollbefugnis der Datenschutzaufsicht allein auf Beschwerdeverfahren lässt sich indessen aus keinem der hier relevanten Gesetze schließen.

Fazit

Die LDI NRW ist vollumfänglich für die Datenschutzkontrolle bei den Staatsanwaltschaften in NRW zuständig und erwartet, dass das Justizministerium dies gegenüber den seiner Aufsicht unterliegenden Staatsanwaltschaften entsprechend klarstellt.

8.3. LDI NRW behält Datenverarbeitung bei der Polizei im Blick

Sammelt die Polizei Daten eines Verdächtigen, darf sie diese nur dann für andere Zwecke weiterverwenden, wenn diese dem Schutz eines ebenso hohen Rechtsguts dienen wie bei der Erstüberwachung. Das hat das Bundesverfassungsgericht bestimmt. Die LDI NRW hat nun überprüft, ob diese Regel auch in das Landespolizeigesetz eingeflossen ist.

Der Weg zu guter Datenverarbeitung ist bisweilen lang. Schon im Jahr 2016 hatte das Bundesverfassungsgericht in seinem Urteil zum Bundeskriminalamtgesetz konkretisiert, dass der polizeilichen Datenverarbeitung durch den Grundsatz der sog. Zweckbindung enge Grenzen gesetzt sind. Daneben macht die JI-Richtlinie der EU bestimmte Vorgaben zur Kennzeichnung polizeilicher Daten. Beide Vorgänge lösten auch in NRW Handlungsbedarf aus und führten zu Anpassungen im Polizeigesetz NRW (PolG NRW). Doch obwohl Zweckbindung und Kennzeichnung für Personen, deren Daten von der Polizei verarbeitet werden, sehr wichtig sind, dauerte es bis ins vergangene Jahr, bis die entsprechenden gesetzlichen Änderungen umgesetzt wurden.

Diese Umsetzung hat die LDI NRW 2024 überprüft – und für grundsätzlich ausreichend befunden. Allerdings wird sie das Thema aufgrund seiner Bedeutung für die polizeiliche Praxis und damit auch für die Grundrechte der Bürger*innen weiter beobachten.

Der Grundsatz der Zweckbindung sichert den Kern des Datenschutzrechts bzw. des Rechts auf informationelle Selbstbestimmung. Er besagt, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden dürfen. Und sie dürfen nur in einer mit diesen Zwecken zu vereinbarenden Weise verarbeitet werden. Insbesondere muss eine Verarbeitung für einen anderen Zweck ebenfalls auf eine Rechtsgrundlage gestützt werden können. Das Ganze muss zudem verhältnismäßig sein.

Dies ist vor allem für die Datenverarbeitung durch Sicherheitsbehörden wichtig, die mit erheblichen Auswirkungen für die Freiheiten der Betroffenen einhergehen kann. Früh stand schon die Frage im Raum, ob einmal rechtmäßig erhobene Daten einfach zu anderen Zwecken weiterverwendet werden dürfen. Das Bundesverfassungsgericht hat dieses Thema in seinem Urteil von 2016 aufgegriffen und die Frage der Zweckbindung bei polizeilicher Datenerfassung näher geprüft. Dabei stellte das Gericht unter anderem klar, dass personenbezogene Daten nur dann für einen anderen Zweck weiterverarbeitet werden dürfen, wenn der neue Zweck mindestens gleichwertige Rechtsgüter schützt, wie der Zweck, für den die Daten ursprünglich erhoben wurden.

Als anschauliches Beispiel dient die Telekommunikationsüberwachung: Diese ist nur zur Abwehr schwerster Gefahren oder zur Aufklärung schwerster Straftaten wie Tötungsdelikte zulässig. Deshalb kommt eine Weiterverarbeitung der erhaltenen Daten nicht in Betracht, wenn sie der Verfolgung eines einfachen Taschendiebstahls dienen soll. Das Rechtsgut Eigentum – vor allem bei geringen Beträgen – ist von geringerem Gewicht als das Rechtsgut Gesundheit oder Leben. Jedenfalls ist der einfache Diebstahl keine schwerste Straftat, für die aber die ursprüngliche Datenerhebung erfolgte. Die Daten dürfen also für die Aufklärung eines Diebstahls nicht genutzt werden.

In der polizeilichen Fachsprache wird diese Vergleichsprüfung „Hypothetische Datenneuerhebung" genannt, abgekürzt HyDaNe. Sie ist notwendig, weil zur Aufklärung schwerster Straftaten auch sehr einschneidend in die Privatsphäre eingegriffen werden kann. So sind in diesen Fällen sogar Maßnahmen wie heimliche Telekommunikationsüberwachung oder gar Wohnraumüberwachung möglich. Dementsprechend dürfen Datenerhebungen, die für die Aufklärung eines Diebstahls gar nicht möglich sind, auch später nicht dafür genutzt werden, wenn sie der Polizei aus Maßnahmen bekannt geworden sind, die der Aufklärung einer schwersten Straftat dienten.

Um die Vorgaben des Bundesverfassungsgerichts in das nordrhein-westfälische Polizeigesetz (PolG NRW) umzusetzen, wurde im Rahmen einer großen Reform im Dezember 2018 § 23 Abs. 2 neu in das Gesetz eingefügt. Er lautet:

> *„2) Die Polizeibehörde kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn*
>
> *1. mindestens*
>
> *a) vergleichbar schwerwiegende Straftaten verhütet oder vorbeugend bekämpft oder*
>
> *b) vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte geschützt werden sollen […]"*

Zusätzlich wurden in § 22b PolG NRW Vorgaben zur Kennzeichnung von Daten festgelegt.

Allerdings wurde für die Umsetzung der Reform eine großzügige Übergangsfrist eingeräumt. Diese ist im Jahr 2024 abgelaufen. Bei der Überprüfung der Umsetzung hat die LDI NRW ihren Fokus zunächst vor allem auf die Herangehensweise der Polizei gelegt. Denn mittlerweile erfolgt die polizeiliche Datenverarbeitung weitgehend digital. Daher waren die rechtlichen Vorgaben in zahlreiche Dateisysteme einzuarbeiten. 2022

hat das Innenministerium NRW dazu eigens eine Arbeitsgruppe eingesetzt, die entsprechend der unterschiedlichen Systeme gesonderte Umsetzungskonzepte entwickelte.

Aus Sicht der LDI NRW ist diese Herangehensweise grundsätzlich tragfähig. Zudem fielen bei einer stichprobenartigen Analyse einzelner Programme keine schwerwiegenden Probleme auf. Lediglich in einem der geprüften Systeme sind die Vorgaben zur Kennzeichnung zu verbessern. Da das Land NRW hierzu auf Änderungen auf Bundesebene angewiesen ist, hat die LDI NRW die Polizei dazu angehalten, auf diese Änderungen hinzuwirken und sie anschließend unverzüglich umzusetzen. Das Innenministerium NRW hat daraufhin bestätigt, auf die Änderung hinzuwirken und ggf. eine Zwischenlösung einzurichten.

Fazit

Bei der stichprobenartigen Überprüfung, ob die Polizei NRW die gesetzlichen Vorgaben bei polizeilichen Datensystemen umsetzt, wurden keine schwerwiegenden Mängel festgestellt. Die LDI NRW wird die Umsetzungsmaßnahmen aber weiter im Blick behalten.

8.4. Polizeibehörden – Finger weg von der WhatsApp-Nutzung!



Unter Polizist*innen in NRW wird offenbar auch über WhatsApp-Gruppen kommuniziert. Doch selbst wenn Behörden oder einzelne Vorgesetzte die Nutzung des Messenger-Dienstes zur Übermittlung von dienstlichen Informationen nur tolerieren, ist das hoch problematisch.

Der Trend zu moderner Kommunikation macht auch vor Behördenmitarbeiter*innen nicht halt. Insbesondere Messenger-Dienste wie WhatsApp sind dabei besonders beliebt. Doch was für private Unterhaltungen hinnehmbar sein kann, stößt im dienstlichen Gebrauch an seine Grenze. Der LDI NRW sind in diesem Zusammenhang 2024 mehrere Beschwerden aus dem Polizeiumfeld in NRW zugetragen worden, die ein Phänomen beschreiben, das aus Datenschutzgesichtspunkten nicht hinzunehmen ist.

Zunächst muss darauf hingewiesen werden, dass Behörden, die Messenger-Dienste für dienstliche Zwecke einsetzen, damit für die Verarbeitung der personenbezogenen Daten (zum Beispiel die Inhalte der Chats, Sprachnachrichten oder Videocalls) verantwortlich werden. Sofern einzelne Vorgesetzte, zum Beispiel Dienstgruppenleitungen bei der Polizei, WhatsApp für die dienstliche Kommunikation verlangen, wird dies der Behörde spätestens dann zugerechnet, wenn ihr bekannt wird, dass die Vorgesetzten den Dienst zur Erfüllung ihrer Vorgesetztenfunktion verwenden.

Nach den der LDI NRW vorliegenden Beschwerden werden bei der Polizei in NRW beispielsweise Anfragen und Mitteilungen zur Veränderung von Dienstplänen über WhatsApp ausgetauscht. Auch wird über Krankmeldungen einzelner Kolleg*innen informiert. Und dabei handelt es sich offenbar nicht um Einzelfälle. Vielmehr wird WhatsApp in vielen Dienstgruppen regelmäßig genutzt. Beschäftigte, die dabei nicht mitmachen, sind von den dienstlichen Informationen weitgehend ausgeschlossen.

All das ist äußerst problematisch, da die betroffenen Beschäftigten veranlasst werden, einen Dienst zu nutzen, der hinsichtlich der Verarbeitung von personenbezogenen Daten intransparent ist. So werden bei Versendung von Nachrichten regelmäßig Metadaten an WhatsApp übermittelt, die sich auf das Nutzungsverhalten der Beschäftigten beziehen, ohne dass die Verwendung dieser Daten geklärt ist.

WhatsApp behält sich außerdem die Erhebung von Telefonnummern mittels Adressbuchupload vom Handy des Mobiltelefonnutzers vor. Das Unternehmen kann auf diese Art alle Kontaktdaten eines Nutzers verarbeiten, die auf dessen Mobiltelefon hinterlegt sind, unabhängig davon, ob der jeweilige Kontakt selbst WhatsApp nutzt oder nicht. Primär soll dies die Kontaktaufnahme mit anderen WhatsApp-Nutzer*innen erleichtern. Über dieses „Match-Making" hinaus nutzt WhatsApp bzw. Meta diese Daten aber auch für eigene Zwecke. Dies ist datenschutzrechtlich nicht zu rechtfertigen, weil die im Adressbuch gespeicherten Personen dazu meist keine Einwilligung erteilt haben – und die veranlassende Behörde keine Rechtsgrundlage dafür hat, solche Verarbeitungsvorgänge zu ermöglichen.

Des Weiteren ist zu bezweifeln, dass die dienstliche Nutzung eines für private Angelegenheiten eingerichteten WhatsApp-Dienstes auf der Basis einer Einwilligung der Behördenmitarbeiter*innen erfolgen kann. Die dazu notwendige Freiwilligkeit einer solchen Einwilligung dürfte kaum gegeben sein. Denn selbst wenn Beschäftigten, die sich an einer WhatsApp-Gruppe nicht beteiligen, andere Informationskanäle zur Verfügung stünden, erzeuge eine innerdienstliche WhatsApp-Gruppe einen Gruppenzwang, der einer freiwilligen Entscheidung im Wege steht. Und noch ein Aspekt ist zu berücksichtigen: Die Unklarheiten über die Datenverarbeitung durch WhatsApp bzw. Meta sind so groß, dass den Beschäftigten sicher nicht alle notwendigen Informationen zur Verfügung gestellt werden können, damit sie abschätzen können, wie ihre Daten verarbeitet werden.

Die LDI NRW hat das Innenministerium NRW auf diesen Missstand und die Möglichkeit hingewiesen, polizeieigene Kommunikationsdienste für den Informationsaustausch zu nutzen. Das Ministerium hat bislang nicht darauf reagiert.

Fazit

Für die dienstliche Nutzung sind WhatsApp und vergleichbare intransparente Messenger-Dienste grundsätzlich unzulässig. Die Leitungen der Dienststellen müssen sicherstellen, dass die datenschutzrechtlichen Vorgaben zum Umgang mit dienstlicher Kommunikation eingehalten werden.

8.5. Verkehrsunfall: Polizei darf Zeugendaten nicht einfach weitergeben



Seit Jahren notieren Polizist*innen in NRW nach einem Verkehrsunfall auch die Daten von Zeug*innen auf der ersten Seite der Unfallmitteilungen – und geben sie so an alle Unfallbeteiligten weiter. Die LDI NRW hat das Landesamt für Zentrale Polizeiliche Dienste auf diese rechtswidrige Praxis aufmerksam gemacht. Mit Erfolg.

Jedes Jahr kommt es zu Hunderttausenden Verkehrsunfällen. 2024 verunglückten allein auf nordrhein-westfälischen Straßen rund 60.000 Menschen, darunter immer wieder auch in Fällen, bei denen etwa Fahrzeuge auf einer Kreuzung zusammenstießen. Doch wer war bei Grün losgefahren und wer bei Rot? Oft kommt es entscheidend darauf an, was unbeteiligte Dritte gesehen haben. Ihre Aussagen sind deshalb von besonderer Wichtigkeit. Zeug*innen genießen besonderen Schutz.

In NRW ist die Polizei jedoch über Jahre deutlich zu nachlässig mit diesem Schutz umgegangen. Grundsätzlich fertigen Polizist*innen bei der Aufnahme von Verkehrsunfällen sog. Unfallmitteilungen an. Dabei wird eine Durchschrift der Seite 1 an die Unfallbeteiligten ausgehändigt. Auf dieser Seite werden die Daten der Unfallbeteiligten festgehalten. Lange Zeit war es aber übliche Praxis, dort zusätzlich auch Zeugendaten aufzunehmen – und diese Daten mit Weitergabe der Durchschrift den Unfallbeteiligten bekannt zu machen.

Für diese Weitergabe der Zeugendaten vor Ort besteht jedoch keine rechtliche Grundlage. Darauf hat die LDI NRW die Polizei aufmerksam gemacht – und 2024 Änderungen entsprechender Regelungen erreicht.

Die Straßenverkehrsordnung legt in § 34 Abs. 1 Nr. 5 fest, dass jede an einem Verkehrsunfall beteiligte Person gegenüber anderen am Unfallort

anwesenden Beteiligten und Geschädigten bestimmte Angaben zu machen hat. Mitzuteilen ist nicht nur, dass man am Unfall beteiligt war. Auf Verlangen sind auch der eigene Name und die eigene Anschrift anzugeben. Zeugen trifft diese Pflicht jedoch nicht. Und das aus gutem Grund: Immer wieder kommt es vor, dass Unfallbeteiligte versuchen, Zeug*innen ausfindig zu machen, zu bedrohen und einzuschüchtern. Dennoch notierten Polizeibeamte in NRW in der Praxis nicht selten Informationen über Zeug*innen auf der Seite 1 der Unfallmitteilungen und gaben sie so an die Unfallbeteiligten weiter.

Eine solche Übermittlung ist aber nur dann zulässig, wenn die Zeugen*innen wirksam hierin eingewilligt haben oder die Übermittlung im Einzelfall auf eine andere Rechtsgrundlage gestützt werden kann. Von Letzterem kann – insbesondere bei Sachschaden – normalerweise nicht ausgegangen werden. In diesen Fällen ist allenfalls eine nachträgliche Datenweitergabe denkbar, beispielsweise, wenn sich eine am Unfall beteiligte Person aufgrund von Problemen bei der Schadensregulierung an die Polizei wendet. Dann kann die Weitergabe im Einzelfall erlaubt sein. Ist hingegen die Weitergabe der Daten von Zeug*innen anlässlich der Unfallaufnahme unzulässig, sind die entsprechenden Personalien der Zeug*innen ausschließlich auf der zweiten – polizeiinternen – Seite der Unfallmitteilung zu vermerken.

Die Polizei NRW hat nach Hinweisen der LDI NRW auf diese Rechtslage ihr Vorgehen angepasst. Sie hat zum einen eine entsprechende Verfügung erlassen, die auf die bestehende Rechtslage hinweist. Zum anderen befindet sich der Runderlass des Innenministeriums NRW vom 25. August 2008 in Überarbeitung, der die Aufgaben der Polizei bei Verkehrsunfällen festlegt (41-61.05.01-3). Das Innenministerium hat zugesagt, die datenschutzrechtlichen Grundsätze hier künftig zu berücksichtigen. Damit einhergehen sollte allerdings, auch den Vordruck der Unfallmitteilung an die korrekte Vorgehensweise anzupassen.

Fazit

Die Polizei NRW hat die Notwendigkeit erkannt, die Unfallaufnahme anders zu gestalten. Sie trägt mit dem Erlass bzw. der angekündigten Überarbeitung entsprechender Regeln dafür Sorge, dass die Rechte der Zeug*innen künftig gewahrt werden. Damit konnte die LDI NRW im Nachgang zum 28. Bericht weitere Verbesserungen bei der polizeilichen Unfallaufnahme erreichen. Sie wird die Entwicklung in diesem Bereich weiterhin im Blick behalten.

8.6. Daten von Zeug*innen sind sensibel – auch wenn es nur um Ordnungswidrigkeiten geht

Zu schnelles Fahren, Missachtung der Vorfahrt oder Falschparken – gerade im Verkehr begehen Bürger*innen immer wieder Ordnungswidrigkeiten. Geahndet werden können diese aber oft erst, wenn Zeug*innen auf den Plan treten. Dabei stellt sich für alle Beteiligten schnell die Frage: Dürfen deren Daten herausgegeben werden, etwa bei Anträgen auf Akteneinsicht? Drei Situationen sind dabei zu unterscheiden.

Das Bearbeiten von Ordnungswidrigkeiten gehört zum Alltag deutscher Behörden. Gerade Verkehrsverstöße, die keine Verkehrsstraftaten sind, wie etwa Falschparken, gefährliches Überholen, falsches Abbiegen oder andere Gefährdungen machen dabei einen Großteil der Arbeit aus. Teil dieser Arbeit ist auch das Beurteilen von Anträgen auf Akteneinsicht der Delinquent*innen, die sich gegen verhängte Bußgelder oder Verwarnungen wehren wollen.

In diesem Zusammenhang müssen die Bearbeiter*innen der Verfahren oft entscheiden, wie sie mit Daten in der jeweiligen Akte umgehen, die von Zeug*innen der Verstöße stammen. Dürfen sie diese überhaupt mit herausgeben? Für die Beantwortung dieser Frage kommt es darauf an, in welchem Stadium sich das Ordnungswidrigkeitsverfahren befindet. Zu unterscheiden ist zwischen dem Bußgeldverfahren auf der einen Seite und dem Verwarnungsverfahren auf der anderen. Außerdem ist noch die Situation zu berücksichtigen, bei der Antragsteller*innen nicht Akteneinsicht begehren, sondern einen datenschutzrechtlichen Auskunftsanspruch geltend machen.

Befindet sich das Verfahren im Stadium des Bußgeldverfahrens, können der betroffenen Person in der Regel auch bestimmte Zeug*innendaten zugänglich gemacht werden. Das Bußgeldverfahren zeichnet sich dadurch aus, dass – nach erfolgter Anhörung – ein Bußgeldbescheid gegen die betroffene Person erlassen wird. Dieser muss auch die entsprechenden Beweismittel enthalten. Gleiches gilt bereits für die Anhörung. Der betroffenen Person soll so eine detaillierte Kenntnis der Beweislage ermöglichen werden, damit sie sich adäquat gegen den Verdacht einer Ordnungswidrigkeit verteidigen kann. Von den Angaben umfasst sind auch Informationen zu Zeug*innen (Name und Wohnort), sofern die Zeug*innen für die Beweisführung benötigt werden und keine berücksichtigungsfähigen Drittschutzinteressen vorliegen – also etwa Umstände, die eine Gefährdung der Zeug*innen bedeuten würden. Diese Regelung findet sich auch in einem Runderlass des Innenministeriums NRW wieder (43.8 - 57.04.16 vom 2. November 2010 – „Verfolgung von Verkehrsverstößen durch die Polizei und Erhebung von Sicherheitsleistungen bei Ordnungswidrigkeiten und Straftaten, Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten durch die Ord-

nungsbehörden”). Allerdings ist darauf zu achten, dass ausschließlich der Nachname der Zeug*in mitzuteilen ist. Dies geht nicht nur auf die Pflicht zur Datensparsamkeit zurück, sondern auch auf den Wortlaut des Erlasses.

Steht hingegen die Nennung von Zeug*innendaten im Verwarnungsverfahren im Raum, gilt anderes. Das Verwarnungsverfahren dient der Ahndung von minderschweren Ordnungswidrigkeiten, also Bagatellen, und stellt eine „vereinfachte” Form des Bußgeldverfahrens dar. Anders als im Bußgeldverfahren findet hier beispielsweise keine vertiefte Aufklärung des Sachverhalts statt und keine Anhörung der betroffenen Person. Das hat für die Delinquent*in erhebliche Vorteile. Da sich der Aufwand des Verfahrens reduziert, verringern sich für die betroffenen Personen auch die zu tragenden Kosten. Im Gegenzug sind deren Rechtsmittel allerdings eingeschränkt. So besteht insbesondere kein Akteneinsichtsanspruch. Für Daten etwaiger Zeug*innen bedeutet das, dass diese nicht mitzuteilen sind. Lediglich ob und wie viele Zeug*innen vorhanden sind, darf offenbart werden. Diese Regelung findet sich ebenfalls in dem oben genannten Erlass des Innenministeriums NRW.

Wehrt sich die Delinquent*in gegen den Vorwurf der Ordnungswidrigkeit, verlässt sie das Verwarnungsverfahren und tritt in das Bußgeldverfahren ein. Dort stehen ihr dann die oben genannten Rechte zu, insbesondere das Recht auf Akteneinsicht mit der Möglichkeit, Name und Anschrift von Zeug*innen zu erhalten.

Die dritte Situation, die mit Blick auf Zeug*innen-Daten eine Rolle spielt, ist der datenschutzrechtliche Auskunftsanspruch. Er wird gegenüber der Ordnungswidrigkeitenbehörde geltend gemacht und gibt der betroffenen Person einen Anspruch darauf, über alle personenbezogenen Daten informiert zu werden, die durch die Behörde über sie verarbeitet werden. Der Anspruch umfasst auch die Information über die Herkunft dieser Daten und damit auch die Auskunft über mögliche Zeug*innen.

Allerdings kann die zu erteilende Auskunft unter bestimmten Voraussetzungen eingeschränkt oder gänzlich unterlassen werden. Dies ist in § 56 des BDSG geregelt. Danach kann eine Aufschiebung, Einschränkung oder Unterlassung soweit und solange erfolgen, „wie andernfalls die Erfüllung der in § 45 BDSG genannten Aufgaben, die öffentliche Sicherheit oder Rechtsgüter Dritter gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt”. Konkret heißt das: Sofern es um Daten von Zeug*innen geht, bedarf es einer Abwägung zwischen den Interessen der Zeug*innen und den Interessen der betroffenen Person. Das Interesse der Delinquent*in besteht darin, sich über Herkunft und Umfang der über sie verarbeiteten personenbezogenen Daten bewusst zu werden und deren Richtigkeit zu überprüfen. Dazu braucht sie eine vollständige Übersicht über diese Daten. Demgegenüber steht das In-

teresse möglicher Zeug*innen, ihre Daten geheim zu halten, um etwaige Repressalien zu vermeiden.

Bei der Abwägung dieser Interessen ist ebenfalls das Verfahrensstadium ausschlaggebend. Während das Interesse der Zeug*innen im Bußgeldverfahren regelmäßig hinter dem der betroffenen Person zurückstehen muss, da die Daten auch durch Akteneinsichtsgesuche eingesehen werden könnten, zeichnet sich im Verwarnungsverfahren ein anderes Bild. Da die Zielrichtung des datenschutzrechtlichen Auskunftsanspruchs nicht die Verteidigungsabsicht der betroffenen Person ist, wiegen die Geheimhaltungsaspekte der Zeug*innen hier schwerer. Informationen über Zeug*innen dürfen nicht weitergegeben werden. Es genügt zur Herkunft der Daten anzugeben, dass sie von einer Privatperson stammen.

Fazit

Vor der Herausgabe von Zeugendaten muss unterschieden werden, in welchem Stadium sich das Ordnungswidrigkeitenverfahren befindet. Im Verwarnungsverfahren sind die Daten für die Delinquent*innen in jedem Fall tabu.

8.7. Fotos von Falschparker*innen aufnehmen? In der Regel ist das ok



Viele Städte und Gemeinden fordern auf ihren Internetseiten dazu auf, Fotos von ordnungswidrig geparkten Kraftfahrzeugen mit erkennbarem Kfz-Kennzeichen einzusenden, damit die Parkverstöße geahndet werden können. Doch dürfen Privatpersonen derartige Fotos überhaupt machen und weitergeben? Die Auffassung der LDI NRW dürfte den Falschparker*innen nicht gefallen.

Sein Fall ging 2024 durch die bundesdeutsche Presse: Der selbsternannte „Anzeigenhauptmeister" fuhr auf seinem Fahrrad durch die Lande und zeigte Falschparker an – nachdem er deren möglichen Parkverstoß fotografiert hatte. Was er tat, führte zu einer intensiven Diskussion darüber, ob ein solches Vorgehen überhaupt erlaubt sei, auch unter Datenschutzgesichtspunkten.

Die LDI NRW hat sich im vergangenen Jahr mit diesen Fragen beschäftigt. Sie hält das Aufnehmen der Autokennzeichen in den meisten Fällen für zulässig.

Bei der Anfertigung, Speicherung und Übermittlung von Fotos von Kfz-Kennzeichen durch Privatpersonen zur Vorlage bei der Ordnungsbehörde, um die Ahndung von Verkehrsverstößen anzuregen, handelt es sich jeweils um die Verarbeitung von personenbezogenen Daten. Hierfür bedarf es einer Rechtsgrundlage nach Art. 6 Abs. 1 der DS-GVO. In Betracht kommt grundsätzlich nur Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO. Hierzu muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein. Außerdem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Als ein solches berechtigtes Interesse gilt das allgemeine Recht auf Anzeige von Straftaten (Erwägungsgrund 50 Satz 9 zur DS-GVO). Zu den Straftraten in diesem Sinn zählen auch Ordnungswidrigkeiten, so dass das Fotografieren von Kfz-Kennzeichen durch Privatpersonen, um die Bilder an die zuständige Ordnungsbehörde zu übermitteln, grundsätzlich auf einem berechtigten Interesse beruht. Eine Ausnahme besteht allerdings dann, wenn etwa offensichtlich keine Straftat oder Ordnungswidrigkeit vorliegt und die Verarbeitung mithin ohne Anknüpfung an einen konkreten Verdacht erfolgt. Auch wenn die Anzeigenerstatter*innen über die Fotodokumentation hinaus weitere Ermittlungen anstellen, zum Beispiel versuchen, anhand des Fotos die Identität der Falschparker*in herauszufinden, dürfte das berechtigte Interesse entfallen. Die Ausübung des Rechts auf Strafanzeige würde dann nicht mehr den eigentlichen Zweck der Verarbeitung von Fotos von Kfz-Kennzeichen darstellen.

Die Verarbeitung muss im Übrigen erforderlich sein. Anzeigenerstatter*innen darf also kein milderes, gleich effektives Mittel zur Verfügung stehen, um die eigenen Interessen zu wahren. Maßgeblich ist dabei, was die Ordnungsbehörde benötigt, um die Anzeige erfolgreich bearbeiten zu können. Fotos gehören in der Regel dazu. Selbst wenn es Zeug*innen gibt, lässt dies die Erforderlichkeit von Fotoaufnahmen nicht ohne Weiteres entfallen. Bildaufnahmen haben meist eine höhere Beweisqualität als Aussagen von Zeug*innen.

Anders kann es im Einzelfall dann sein, wenn es des übermittelten Fotos eines Kfz-Kennzeichens nicht bedarf, um die Verfolgung durch die zuständige Ordnungsbehörde zu ermöglichen. So wird die Erforderlichkeit der Ablichtung dann abzulehnen sein, wenn für die Anzeige erstattende Person erkennbar ist, dass die Polizei den Parkverstoß bereits aufnimmt.

Schließlich erfordert Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO eine Interessenabwägung. Dabei kann regelmäßig davon ausgegangen werden, dass die Interessen der Anzeige erstattenden Person die entgegenstehenden Interessen der das Fahrzeug haltenden Person überwiegen. Zu berücksichtigen ist insbesondere, dass Straßenverkehrsteilnehmende mit Bildaufnahmen ihrer verbotswidrig abgestellten Fahrzeuge rechnen müssen – und zwar auch dann, wenn der konkrete Parkverstoß nicht zu einer Beeinträchtigung der Anzeigenerstatter*in führt. Wer falsch parkt, muss eine solche Datenverarbeitung erwarten. Eine Grenze bilden Fälle, in denen einzelne Personen sich die Funktion der Ordnungsbehörde anmaßen und systematisch nach Ordnungsverstößen suchen. Ein solches Handeln würde die Grenze dessen überschreiten, womit Betroffene rechnen müssen. Wir hatten den eingangs erwähnten Fall des Anzeigenhauptmeisters nicht zu prüfen. Er scheint an dieser Grenze zu liegen.

Fazit

Falschparker*innen werden durch den Datenschutz nicht vor der Ahndung von Parkverstößen geschützt. Fertigen Privatpersonen Fotos von Kfz-Kennzeichen an, um diese an die Ordnungsbehörde zu übermitteln, ist dies in den allermeisten Fällen zulässig.

8.8. Helfer*innen auf Großveranstaltungen dürfen nicht einfach reihenweise von der Polizei durchleuchtet werden

Veranstaltungen wie etwa die Fußball-Europameisterschaft 2024 funktionieren nur durch den Einsatz vieler helfender Hände. Das erhöht aber zugleich das Sicherheitsrisiko. Um dieses zu minimieren, wurden in NRW die bei der EURO 2024 eingesetzten Personen durch Abfragen über Erkenntnisse bei Polizei- und Verfassungsschutzbehörden überprüft. Ein derart intensiver Grundrechtseingriff erfordert jedoch eine spezielle gesetzliche Grundlage – die in NRW fehlt.

Die Fußball-Europameisterschaft in Deutschland, die im vergangenen Jahr auch in Stadien in NRW ausgetragen wurde, verlief zum Glück weitgehend friedlich. Sicherheit auf der EURO 2024 wurde großgeschrieben – und dafür in NRW auch auf eine Maßnahme zurückgegriffen, die eine Vielzahl von Menschen erfasste. Um das Gefahrenpotenzial gering zu halten, wurden die vielen Helfer*innen bei den Spielen, in den Stadien und drumherum von der Polizei NRW intensiv durchleuchtet. Im Rahmen der Akkreditierung kam es zu einer massenhaften Überprüfung bei den deutschen Sicherheitsbehörden.

War das rechtens? Darf dieses Mittel zukünftig für weitere Großveranstaltungen eingesetzt werden? Derartige Fragen drängen sich auf, schließlich kommt es zum Abruf teils sensibelster Daten von Polizei und Verfassungsschutz, was für die Betroffenen einen nicht unerheblichen Eingriff in ihre Grundrechte bedeutet. Die LDI NRW sieht hier ein erhebliches datenschutzrechtliches Problem. Solche Eingriffe durch den Staat und seine Behörden erfordern immer eine ausdrückliche gesetzliche Grundlage. In NRW werden die Überprüfungen bislang jedoch allein auf Basis von Einwilligungen der Betroffenen durchgeführt. Und das ist nicht ausreichend.

Damit die Einwilligung wirksam ist, muss sie freiwillig erfolgen. Dies setzt eine echte Wahlfreiheit der Betroffenen voraus. Hieran mangelte es in vielen Akkreditierungsfällen jedoch, da das Weiterbestehen oder Eingehen von Beschäftigungsverhältnissen von dem Einverständnis der betroffenen Personen abhängig ist. Kurz gesagt: Wer der Verarbeitung seiner Daten nicht zustimmte, wurde nicht als Helfer*in zugelassen.

In einer solchen Konstellation kann von Freiwilligkeit aber keine Rede mehr sein. Auch der Bundesdatenschutzbeauftragte warnt in seinem 32. Tätigkeitsbericht die Bundesbehörden, auf eine derartige unzulässige Verarbeitung von Daten bei Großveranstaltungen zurückzugreifen.

Erforderlich ist vielmehr eine ausdrückliche Rechtsgrundlage, in der unter anderem klar geregelt ist, welche Datenverarbeitungen Sicherheitsbehörden im Zusammenhang mit gefährdeten Großveranstaltungen durchführen dürfen. Die Problematik der fehlenden Rechtsgrundlage betrifft nicht nur die EURO 2024, sondern jede andere Großveranstaltung wie beispielsweise große Musikfestivals, von denen in NRW jährlich viele stattfinden.

Bereits 2019 hat die LDI NRW die Landesregierung NRW darauf aufmerksam gemacht, dass die reine Einholung von Einwilligungen in diesem Kontext unzureichend und eine Vielzahl der vorgenommenen Datenverarbeitungen unzulässig sei. Das Innenministerium NRW hatte damals signalisiert, Handlungsbedarf erkannt zu haben und wiederholt zugesichert, eine Rechtsgrundlage zu schaffen. Selbst die Polizei sprach anlässlich der EURO 2024 in einer Bund-Länder Projektgruppe der Polizei die deutliche Empfehlung aus, eine spezialgesetzliche Rechtsgrundlage für die Durchführung von polizeilichen Zuverlässigkeitsüberprüfungen zu erlassen.

Geschehen ist bis heute nichts. NRW ist mittlerweile eines der letzten Bundesländer ohne eine entsprechende Regelung. Zwischenzeitlich ist das Innenministerium sogar ausdrücklich von seiner früheren Zusage abgerückt, eine Norm schaffen zu wollen.

Fazit

Solange in NRW keine ausreichende Rechtsgrundlage geschaffen wird, ist die Überprüfung von Helfer*innen und Mitarbeiter*innen auf Großveranstaltungen in NRW in vielen Fällen rechtlich nicht zulässig. Die LDI NRW sieht hier dringenden Handlungsbedarf für die Landesregierung. Das Innenministerium NRW wurde über die Problematik informiert, ist bislang aber nicht tätig geworden.

8.9. Corona-Hilfen: Fluten mit Auskunftsanträgen macht einzelnen Antrag nicht automatisch rechtsmissbräuchlich



Im Streit um die Rückforderung der „NRW Soforthilfe 2020" haben betroffene Bürger*innen das Land mit Auskunftsanträgen zur Verarbeitung ihrer Daten überzogen. Ist so etwas zulässig? Die LDI NRW findet: grundsätzlich ja. Und sie rät den Behörden, sich für eine solche Antragsflut gut zu rüsten.

Die Pandemie ist vorbei, die Abwicklung aber läuft noch immer – insbesondere auch mit Blick auf finanzielle Fragen. Wurden anfänglich auch in NRW recht unbürokratisch Gelder als Corona-Hilfen an in Not geratene Unternehmen und Selbstständige ausgegeben, sahen sich diese später teilweise mit Rückforderungen durch das Land konfrontiert. Zahlreiche Rechtsstreitigkeiten waren die Folge.

Auch die LDI NRW musste sich 2024 erneut mit dem Thema befassen. Grund dafür war der Aufruf einer Interessengemeinschaft, die rückfordernde Landesregierung mit Anträgen auf Auskunft über die Verarbeitung personenbezogener Daten zu fluten. Doch die Einschätzung des zuständigen Wirtschaftsministeriums, die Bearbeitung der jeweiligen Anträge deshalb als missbräuchlich anzusehen und nicht zu bearbeiten, konnte von der LDI NRW nicht mitgetragen werden.

Begonnen hatte die Auseinandersetzung mit einem Urteil des Oberverwaltungsgerichts NRW (OVG NRW). Das entschied im März 2023, dass Corona-Hilfen, welche den Finanzbedarf der Empfänger*innen überstiegen, zurückgefordert werden dürfen. Die bisherige Praxis der Rückforderung erklärten die Richter allerdings für gesetzeswidrig (OVG NRW, Urteile vom 17. März 2023, Az. 4 A 1986/22, 4 A 1987/22, 4 A 1988/22). Daraufhin übernahm das Wirtschaftsministerium NRW federführend die Aufgabe,

die Rückforderungen in Form eines Verwendungsnachweisverfahrens neu zu organisieren.

Die Betroffenen reagierten Anfang Juni 2023 mit einer Flut von Auskunftsanträgen. Die „IG-NRW Soforthilfe", eine Interessengemeinschaft von Empfänger*innen der Corona-Hilfe, hatte ihre Mitglieder aufgerufen, gegenüber dem Wirtschaftsministerium NRW Ansprüche nach Art. 15 der DS-GVO geltend zu machen. Art. 15 DS-GVO gibt Bürger*innen, deren personenbezogene Daten verarbeitet wurden, unter anderem das Recht, von dem Verantwortlichen Auskunft über diese Daten zu verlangen.

Auf der Internetseite der Interessengemeinschaft wurde ein entsprechendes Musterantragsformular bereitgestellt. In einem Mitgliederforum bei Facebook wurde zudem als Ziel des Aufrufs verbreitet, „[…] NRW bei seinen weiteren Bearbeitungen noch etwas auf[zuhalten], sie sollen ja nicht unbedingt schnell fertig werden mit dem neuen ‚Verwendungsnachweisverfahren'. Abgesehen davon, dass wir ‚Rechte' haben […] Ok, es ärgert sie auch maßlos, klar". Bis September 2023 gingen 926 Antragsschreiben mit einem von der IG-NRW Soforthilfe bereitgestellten Musterformular beim Ministerium ein, das zuvor von dem Aufruf erfahren hatte.

Das Wirtschaftsministerium NRW bat die LDI NRW um Beratung, ob die Auskunftsersuchen wegen der Zielsetzung des Aufrufs als rechtsmissbräuchlich abgelehnt werden könnten. Mit einer solchen Antragsflut habe das Ministerium nicht gerechnet. Der Bearbeitungsaufwand sei gravierend. Wie von den Antragsteller*innen beabsichtigt, sei es für das zuständige Referat unmöglich, die Anträge in der dafür vorgesehenen Monatsfrist zu beauskunften und gleichzeitig das neue Rückmeldeverfahren planmäßig fertigzustellen.

Die LDI NRW aber konnte dem Ministerium nur empfehlen, die Anträge zu beauskunften. Denn welche Motivation einzelne Antragsteller*innen verfolgen, kann allein aufgrund eines solchen Aufrufs nicht festgestellt werden. Jede einzelne Person hat einen Anspruch nach Art. 15 DS-GVO. Ein erstmaliger und bis dahin einmaliger Auskunftsantrag ist dementsprechend nicht missbräuchlich. Zudem konnte dem Aufruf keine Störungsabsicht als alleiniges Ziel entnommen noch den einzelnen Antragsteller*innen nachgewiesen werden.

Das Ministerium wurde zugleich darüber informiert, dass wegen der unvorhersehbar hohen Zahl an Anträgen die Bearbeitungsfrist um zwei Monate verlängert werden kann und dass die Betroffenen darüber innerhalb eines Monats nach Antragseingang zu unterrichten sind (Art. 12 Abs. 3 DS-GVO). Da die Anträge nicht auf das Soforthilfeverfahren beschränkt waren, hatten grundsätzlich alle Abteilungen im Wirtschaftsministerium zu prüfen, ob dort Daten über die Antragsteller*innen vorliegen. Nach

§ 12 Abs. 1 DSG NRW konnten zum Auffinden weiterer, über das Soforthilfeverfahren hinausgehender Daten aber weitere Anhaltspunkte bei den Betroffenen angefordert werden.

Zunächst hielt das Ministerium trotzdem an der Einschätzung fest, dass die Auskunftsbegehren missbräuchlich seien und lehnte die Anträge ab. Die LDI NRW musste deshalb – und weil sie zahlreiche Beschwerden erhielt – als Aufsichtsbehörde einschreiten. Am Ende lenkte das Ministerium ein und erteilte den Betroffenen die verlangten Auskünfte.

Zwar ist der Unmut des Wirtschaftsressorts durchaus nachvollziehbar, denn dort liegt der Fokus auf der Erledigung der Sachaufgabe, also des Rückforderungsverfahrens. Allerdings ist das Auskunftsrecht das zentrale Recht für Betroffene, um sich über die Daten zu vergewissern, die über die eigene Person verarbeitet werden. Gerade in inzwischen lange laufenden Förderverfahren, ist es nicht abwegig, wenn Betroffene noch einmal die Angaben prüfen wollen, die sie bei der Antragstellung gemacht haben. Dies kann für die Beurteilung der Rechtmäßigkeit eines zu erwartenden Rückforderungsbescheides sogar sehr relevant sein. Deswegen ist eine pauschale Annahme, die Antragsteller*innen handelten allesamt primär in Schädigungsabsicht, nicht möglich. Welches Motiv jede einzelne Person für den Antrag hatte, war nicht belegbar. Die Pflicht zum Nachweis des missbräuchlichen Charakters des Auskunftsbegehrens lag beim Wirtschaftsressort. Im Regelfall ist ein erst- und einmaliger Auskunftsantrag einer einzelnen Person nicht missbräuchlich. Das ist die klare Botschaft auch der Rechtsprechung zu diesem Thema.

Verantwortliche stehen in der Pflicht, Verfahren zur Verarbeitung personenbezogener Daten so einzurichten, dass Betroffenenrechte erfüllt werden können. Nach den Erfahrungen bei der NRW Soforthilfe 2020 sollten Behörden, die Berührungspunkte zu Massenverfahren mit einer Vielzahl gleichgelagerter Verwaltungsvorgänge haben, mit Situationen rechnen, in denen sie mit außergewöhnlichen Antragshäufungen konfrontiert sind. Auf den Einwand des Rechtsmissbrauchs können sich die Behörden dabei nur in seltenen Fällen berufen. Es ist daher notwendig, technisch-organisatorische Vorkehrungen zu treffen, um auch bei vielen Anträgen in kurzer Zeit den Anforderungen der DS-GVO gerecht werden zu können. Auch sollte die Möglichkeit von Auskunftsersuchen bei der elektronischen Aktenführung von vornherein mitgedacht werden. Das kann bei späteren Anfragen hilfreich sein. Das schnelle Auffinden und Bereitstellen von Daten lasse sich sowohl durch Möglichkeiten zur sicheren Schwärzung nicht relevanter Daten als auch durch die Berücksichtigung der Namen von Verfahrensbeteiligten bei der Stichwortvergabe erreichen.

Fazit

Die Annahme eines Missbrauchs des Auskunftsrechts kann nicht allein darauf gestützt werden, dass eine Vielzahl von Personen einem Aufruf zur Stellung von Auskunftsanträgen folgt. Die Verwaltung ist gut beraten, ihre Daten so zu ordnen, dass Auskunftsrechte schnell erfüllt werden können, selbst bei einem Bezug zu Massenverfahren. Die Verwaltung sollte die hierfür notwendigen technisch-organisatorischen Vorkehrungen im Voraus treffen.

9. Gesundheit und Soziales



9.1. Die Pandemie ist vorbei, die Missachtung des Datenschutzes geht weiter

Manche Testzentren-Betreiber arbeiteten schon während der Corona-Pandemie nicht datenschutzkonform. Aber auch danach zeigt sich: Im Umgang mit Datenlöschanträgen fehlt es an Zuverlässigkeit, teilweise werden Daten zu Werbezwecken missbraucht. Dabei können die Strafen durchaus empfindlich ausfallen.

Der Corona-Virus ist nicht weg, aber die Pandemie ist vorbei, und mit ihr haben sich auch die vielerorts entstandenen Testzentren aufgelöst. Geblieben sind allerdings datenschutzrechtliche Probleme, die sich schon in der Hochphase der Pandemie gezeigt hatten. Waren es in den ersten Jahren nicht oder verspätet erteilte datenschutzrechtliche Auskünfte durch Testzentren-Betreiber*innen, musste sich die LDI NRW im vergangenen Jahr zusätzlich mit fehlender Datenlöschung und unberechtigter Datennutzung beschäftigen. Dabei hat sich gezeigt: ohne Bußgelder geht es offenbar nicht.

Im Fokus standen insbesondere die persönlichen Informationen, die Menschen, welche sich beim Testzentrum angemeldet hatten, beim Besuch dort hinterlassen haben. Teilweise wurden sie zweckentfremdet, in einem anderen Fall nicht gelöscht.

Im ersten Fall hatten sich mehrerer Bürger*innen über einen ehemaligen Betreiber eines Coronavirus-Testzentrums beschwert. Der hatte die während des Betriebs erhobenen E-Mail-Adressen der Besucher*innen nach Schließung des Testzentrums genutzt, um ihnen Werbung zu schicken – für einen neuen, von ihm an Ort und Stelle des ehemaligen

Testzentrums betriebenen Schnellimbiss. Ein solches Vorgehen ist jedoch eindeutig rechtswidrig.

So fehlt es an der notwendigen Rechtsgrundlage für die Verwendung der Daten. Personenbezogene Daten, wie private E-Mail-Adressen, sind auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten. Außerdem gilt im Datenschutzrecht der Grundsatz der Zweckbindung. Daten dürfen danach nicht in einer mit dem (legitimen) Zweck der Erhebung nicht zu vereinbarenden Weise weiterverarbeitet werden.

Im konkreten Fall ist dies jedoch geschehen. Die Besucher*innen hatten ihre E-Mail-Adressen hinterlegt, damit ihnen das Testergebnis mitgeteilt sowie diese bei einem etwaig positiven Testergebnis an das zuständige Gesundheitsamt weitergeben wurde. Es ging ihnen nicht darum, über die E-Mail-Adressen später auch Werbung des Betreibers zu erhalten. Eine Verbindung zwischen dem ursprünglichen Zweck, für den die E-Mail-Adressen erhoben wurden, und dem Zweck der Weiterverarbeitung in Form von Werbung, bestand folglich nicht. Die Weiterverarbeitung war für die betroffenen Personen auch nicht erwartbar noch konnte man ihnen unterstellen, dass sie die Weiterverarbeitung billigend in Kauf genommen hätten. Dafür sind der Betrieb einer Coronavirus-Teststelle und derjenige eines Imbisses erkennbar zu unterschiedlich.

Einwilligungen der Betroffenen in die Weiterverarbeitung ihrer Daten lagen schließlich ebenfalls nicht vor. Ebenso wenig war die Weiterverarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich. Jedenfalls überwogen vorliegend die Interessen der betroffenen Personen an einem Unterlassen der werblichen und damit zweckwidrigen Nutzung der privaten E-Mail-Adressen. Die LDI NRW hat gegen den ehemaligen Testzentrums-Betreiber am Ende ein Bußgeld verhängt.

Das gleiche gilt für den zweiten Fall, bei dem der Betreiber Auskunfts- und Löschungsansprüche missachtet hatte.

Grundsätzlich verlangt die DS-GVO, dass der Verantwortliche einer Datenverarbeitung binnen eines Monats auf Löschanträge oder Auskunftsersuchen von betroffenen Personen reagiert. Auch wenn kein Löschanspruch besteht, ist dies dem Betroffenen innerhalb der Frist mitzuteilen. Die Betriebsabläufe sind so zu gestalten, dass die Erfüllung dieser Pflichten sichergestellt ist.

Eine bundesweit tätige Betreiberin von Testzentren hatte damit offenbar so ihre Probleme. Wegen nicht und verspätet erteilter datenschutzrechtlicher Auskünfte hatte die LDI NRW bereits in den Jahren 2021, 2022 und 2023 in drei Fällen Bußgelder gegen sie verhängt. Im vergan-

genen Jahr dann musste sich die LDI NRW erneut mit der Betreiberin befassen.

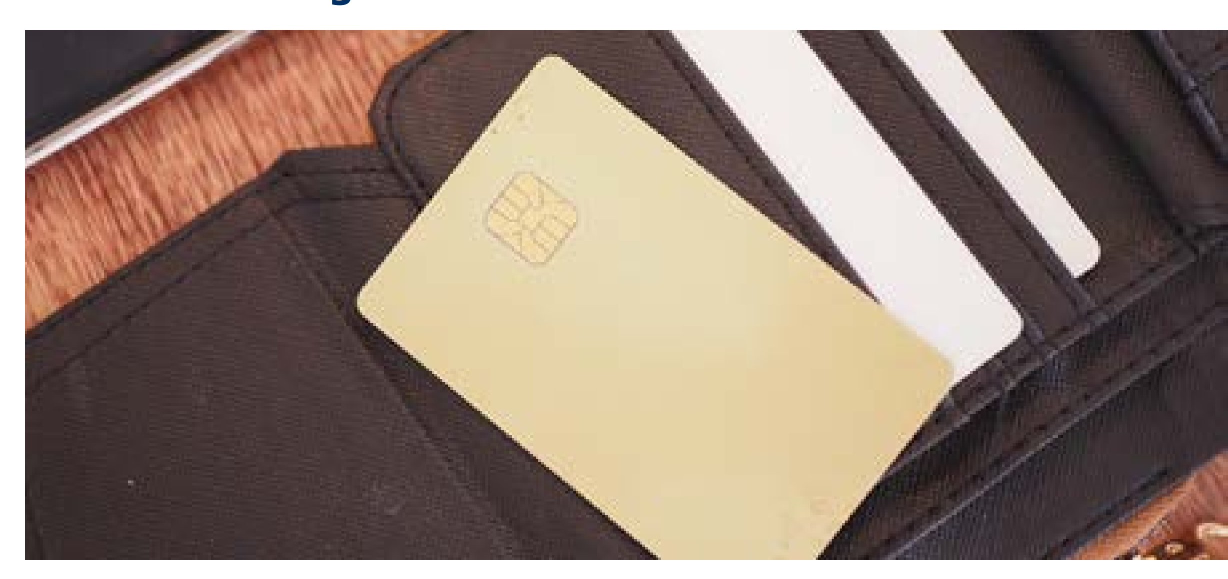
Der Besucher einer ihrer Testzentren hatte die Betreiberin via E-Mail zur Löschung seiner personenbezogenen Daten aufgefordert, von dieser aber keine Reaktion erhalten. Im daraufhin eingeleiteten aufsichtsbehördlichen Verfahren erklärte die Betreiberin dann, sie habe auch nach erneuter Prüfung aller Eingänge keinen Löschantrag des Beschwerdeführers finden können. Der konnte jedoch nachweisen, auf seine E-Mail sowohl eine automatisch generierte Eingangsbestätigung als auch eine weitere E-Mail-Antwort der Betreiberin erhalten zu haben. Darin wurde er über eine Weiterleitung an die zur Bearbeitung „zuständige Abteilung" informiert.

Für die Betreiberin wurde es daraufhin teuer. Unter Berücksichtigung der bereits in der Vergangenheit ergangenen Bußgeldentscheidungen und der Tatsache, dass die Betreiberin ihr Management von Betroffenenrechten trotz entgegenstehender Beteuerungen weiterhin nicht im Griff hat, verhängte die LDI NRW dieses Mal ein Bußgeld in fünfstelliger Höhe.

Fazit

Die Weiterverarbeitung rechtmäßig gespeicherter E-Mail-Adressen muss mit dem ursprünglichen Erhebungszweck vereinbar sein. Eine zu Werbezwecken erfolgte Nachnutzung der bei einem Testzentrum gespeicherten E-Mail-Adressen von Besucher*innen ist das nicht und deshalb ohne deren Einwilligung unzulässig. Die Erfüllung datenschutzrechtlicher Betroffenenrechte wie Auskunfts- und Löschungspflichten gehört darüber hinaus zu den Kardinalpflichten von Datenverarbeiter*innen. Sie müssen ihren Betriebsablauf so gestalten, dass die vollständige und rechtzeitige Erfüllung dieser Pflichten unternehmensweit sichergestellt ist.

9.2. Bezahlkarte für Geflüchtete: Diese wichtigen Punkte müssen bei der Einführung beachtet werden



Auch in NRW wird eine Bezahlkarte kommen, die weitestgehend Bargeldauszahlungen an Geflüchtete ersetzt. Die LDI NRW begleitet die datenschutzkonforme Einführung – und hat bestimmte Kriterien identifiziert, die bei der Einführung im Blick bleiben müssen.

Das Thema Migration war 2024 eines der beherrschenden politischen Themen in Deutschland. Neben Fragen der Aufnahmekapazitäten von Geflüchteten und Abschiebemöglichkeiten stand dabei die sog. Bezahlkarte im Mittelpunkt. Durch Änderung des Asylbewerberleistungsgesetzes (AsylbLG) vom 16. Mai 2024 wurde schließlich diese veränderte Möglichkeit der Leistungsgewährung an Geflüchtete geschaffen. Ihre konkrete Ausgestaltung obliegt jeweils den Ländern. In NRW ist die landesweite Einführung im Frühjahr 2025 geplant. Wo die Karte eingeführt wird, müssen Geflüchtete statt mit Bargeld seither mit dieser Karte bezahlen.

Die LDI NRW hat die Einführung der Bezahlkarte von Anfang begleitet, damit die Umsetzung datenschutzkonform erfolgt. So hat die LDI NRW in länderübergreifenden Gremien wichtige Impulse nicht nur für die Leistungsbeschreibung im Vergabeverfahren gegeben, sondern auch für eine zu erstellende Datenschutzfolgeabschätzung. Außerdem wurde das Positionspapier der DSK mit dem Titel „Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem AsylbLG" maßgeblich mitgestaltet.

Dabei wurden zahlreiche Kriterien identifiziert, die bei der Gestaltung der Bezahlkarte unbedingt beachtet werden müssen:

- Den Leistungsbehörden darf keine Möglichkeit eingeräumt werden, den Guthabenstand der Leistungsberechtigten ohne deren aktive Mitwirkung einzusehen.

- Es ist sehr bedenklich, sollte die Nutzung der Bezahlkarte pauschal auf bestimmte Postleitzahlengebiete innerhalb des Bundesgebiets beschränkt werden. Auf diese Weise könnten Dritten mögliche Wohnsitzauflagen bekannt werden, die für die kartennutzende Person gelten.

- Die Datensätze der anspruchsberechtigten Personen, die bei den einzelnen Leistungsbehörden bestehen, sind bei einem Dienstleister, der die Bezahlkarte für eine Vielzahl von Leistungsbehörden anbietet, strikt voneinander zu trennen.

- Eine Weitergabe der Ausländer-Zentralregisternummern der Leistungsberechtigten an den Dienstleister ist auszuschließen, da diese für dessen Aufgabenerfüllung nicht erforderlich sind.

- Zugriffe auf Buchungsdaten durch Sicherheitsbehörden sind nur nach den gesetzlichen Maßgaben der einschlägigen Sicherheitsgesetze zulässig, zum Beispiel der Strafprozessordnung, die auch für andere Personen und deren Bankaktivitäten gelten.

Die LDI NRW hat außerdem an einer Anhörung des Integrationsausschusses des Landtags teilgenommen und eine schriftliche Stellungnahme (18/2139) zu dem Gesetzentwurf abgegeben, mit dem die Rechtsgrundlage für die Einführung der Bezahlkarte in NRW geschaffen wird (Zweites Änderungsgesetz zur Ausführung des AsylbLG). Hier hat die LDI NRW besonders begrüßt, dass Kommunen keinem Zwang zur Einführung der Bezahlkarte unterliegen. Es ist ein Gebot der Verhältnismäßigkeit, dass Kommunen, die keine Anhaltspunkte für Missbrauch von Asylleistungen in ihrem Zuständigkeitsbereich feststellen, die Möglichkeit haben, die Bezahlkarte nicht einzusetzen.

Fazit

Bei der Einführung der Bezahlkarte für Geflüchtete sind sämtliche Datenverarbeitungsprozesse von den verantwortlichen Stellen zu beachten. Dies betrifft nicht nur deren rechtliche Zulässigkeit, sondern ebenso eine Einschätzung der möglichen Risiken dieser Datenverarbeitungen und die Implementierung entsprechender geeigneter Schutzmaßnahmen.

9.3. Auskunft vom Jugendamt? Eltern haben hier nur eingeschränkte Rechte

Wenn Vätern oder Müttern das Sorgerecht entzogen wird, möchten diese häufig wissen, welche Daten das Jugendamt über sie speichert. Und sie wollen prüfen, ob die Tatsachen zutreffen, die den Sorgerechtsentzug begründen. In der Regel stehen einem umfassenden Auskunftsanspruch aber die Datenschutzrechte der anderen Familienmitglieder entgegen.

Nach einem Sorgerechtsentzug verlieren betroffene Eltern oft das Vertrauen in das Jugendamt und das Familiengericht. Auskünften des Jugendamts wird kein Glauben mehr geschenkt. Das Vertrauen ist mitunter so zerstört, dass jegliche Auskunft abgelehnt wird, die hinter einer vollständigen Kopie der Kindesakte zurückbleibt.

Häufig kommt es vor, dass Eltern dann Anträge zu Informationen aus der Akte des Kindes wieder und wieder stellen – mit dem Ziel, so eine vollständige Auskunftserteilung zu erreichen. Dies stellt die Jugendämter nicht nur wegen des Umfangs der Akten, sondern auch wegen des nicht enden wollenden Schriftwechsels vor erhebliche Probleme. Dabei ist die Lage nach dem Datenschutzrecht weitgehend klar.

Tatsächlich zeigen die Erfahrungen der LDI NRW, dass die Jugendämter in NRW grundsätzlich bereit und bemüht sind, Anfragenden zu ihren eigenen Daten im Rahmen des Möglichen Auskunft zu erteilen. Allerdings sind ihnen dabei rechtliche Grenzen gesetzt. Zunächst gilt, dass Eltern, denen das Sorgerecht entzogen wurde, nicht mehr befugt sind, in Vertretung des Kindes Auskunft über Daten des Kindes zu verlangen. Sie können nur Auskunft über die eigenen Daten beantragen, die in der Jugendamtsakte enthalten sind. Dem stehen aber meist Rechte Dritter entgegen. So scheitert die Herausgabe einer vollständigen Kopie der Akte in der Regel daran, dass sie auch Daten über das Kind, das andere Elternteil oder andere in die Betreuung des Kindes eingebundener Personen enthält. Die Rechte und Freiheiten all dieser Beteiligten muss das Jugendamt in gleichem Maße achten wie die Rechte des die Auskunft verlangenden Elternteils.

Das Recht auf Auskunft zu den eigenen Daten ist vor allen Dingen dann eingeschränkt, wenn Sozialdaten den Mitarbeitenden eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut wurden. Hier gewichtet die gesetzliche Wertung in § 65 des Sozialgesetzbuchs (SGB) VIII zusammen mit § 35 des SGB I die Interessen der sich anvertrauenden Person immer höher als das Recht der Person, die Auskunft verlangt.

Es handelt sich dabei um eine gesetzliche Einschränkung des Auskunftsanspruchs gemäß Art. 23 Abs. 1 Buchstabe e der DS-GVO. Sie soll die soziale Sicherheit und den Schutz der Rechte insbesondere jener Kinder und Jugendlichen gewährleisten, die durch die Jugendhilfe betreut werden. Kinder und Jugendliche sowie Personen, die mit den Kindern umgehen, können sich nur dann der Jugendhilfe anvertrauen, wenn sie sicher sein können, dass ihre Informationen nicht weitergegeben werden. Nur durch die Aufrechterhaltung eines geschützten Bereichs wird die Jugendhilfe in die Lage versetzt, die Informationen zu erhalten, die sie für die soziale Unterstützung der Kinder und Jugendlichen benötigt.

Vertrauen Kinder oder Jugendliche der Jungendhilfe beispielsweise Informationen zu einem Kindesmissbrauch oder eine Misshandlung durch ein Elternteil an, müssen sie sicher sein können, dass diese Informationen nicht an das betroffene Elternteil herausgegeben werden. Hier überwiegt der Schutz der sich anvertrauenden Person regelmäßig das Auskunftsrecht der Person, auf die sich die anvertrauten Informationen beziehen.

Eine Weitergabe der Informationen kommt ausnahmsweise nur unter den engen Voraussetzungen des § 65 SGB VIII in Betracht – wenn etwa eine Einwilligung der Person vorliegt, welche die Daten anvertraut hat. Handelt es sich dabei um ein Kind, kann die Einwilligungsfähigkeit aber altersbedingt eingeschränkt sein mit der Folge, dass das sorgeberechtigte Elternteil bei der Einwilligung mitwirken müsste. In Fällen, in denen die Ehepartner nicht mehr miteinander klarkommen, ist dies häufig ein Problem, das aber das Datenschutzrecht nicht lösen kann.

Erhält die LDI NRW Beschwerden über eine nicht erteilte Auskunft, wird das jeweils betroffene Jugendamt zunächst um einen Bericht gebeten. In aller Regel liefern die angeschriebenen Ämter eine nachvollziehbare Begründung, warum bestimmte Daten nicht herausgegeben werden können. Die LDI NRW informiert daraufhin diejenigen, die sich beschwert haben darüber, dass ihr Auskunftsanspruch aufgrund der Rechte Dritter nur eingeschränkt besteht. Betroffene verfolgen trotzdem oft sehr hartnäckig ihre Forderung nach einer vollständigen Kopie der Jugendamtsakte ihres Kindes weiter.

Das hat auch damit zu tun, dass in dieser Phase zwischen den Eltern längst unterschiedliche Ansichten über das Verhalten des jeweils anderen bestehen und dies in der Jugendamtsakte dokumentiert ist. Der Datenschutzanspruch wird dadurch oftmals zum Nebenkriegsschauplatz. Das Datenschutzrecht ist aber nicht geeignet, unterschiedliche Wahrnehmungen der Familienmitglieder zu Trennungsgründen und deren Auswirkungen auf die Kinder zu klären. Die LDI NRW kann dann nur noch auf die familienrechtlichen Verfahren und die Wahrnehmung von möglichen Rechten in diesem Rahmen verweisen.

Fazit

Unterschiedliche Sichtweisen auf familieninterne Ereignisse durch die Betroffenen können nicht durch Datenschutzrechte befriedet oder gar geklärt werden. Das Beharren auf einer vollständigen Kopie der Kindesakte führt nicht zum Ziel und kann von der LDI NRW aufgrund der gesetzlichen Rahmenbedingungen nicht unterstützt werden.

9.4. Telefonnummer und E-Mail-Adresse müssen beim Jobcenter nicht angegeben werden

In den Online-Formularen eines Jobcenters erfolgt die Preisgabe von Telefonnummer und E-Mail-Adresse stets freiwillig. Werden antragstellende Personen dazu verpflichtet, stellt das einen Datenschutzverstoß dar.

Kaum eine Dienstleistung, die heutzutage nicht online beantragt werden kann. Das gilt auch für Erst- und Weiterbewilligungsanträge für Bürgergeld, die bei den kommunalen Jobcentern gestellt werden können. Doch wie so oft liegt in punkto Datenschutz der Teufel im Detail, etwa bei den persönlichen Angaben, die in den Anträgen verlangt werden. So musste sich die LDI NRW 2024 mit einem Fall beschäftigten, bei dem eines der kommunalen Jobcenter in seinen Formularen die Angabe von Telefonnummer und E-Mail-Adresse der Antragstellenden für verpflichtend erklärt hatte. Das jedoch ist ein klarer Verstoß gegen das Datenschutzrecht.

So ist im Gesetz (§ 67 Abs. 1 Zehntes Buch SGB) eindeutig geregelt, dass Sozialdaten nur dann zulässigerweise erhoben werden dürfen, wenn die erhebende Stelle ohne diese Kenntnis ihre Aufgabe nicht erfüllen kann.

Diese Voraussetzung ist für Telefonnummer und E-Mail-Adresse bei einem Antrag auf Bürgergeld aber nicht gegeben. Diese Grundsicherung für Arbeitssuchende umfasst Leistungen zur Beratung, Beendigung oder Verringerung der Hilfebedürftigkeit, insbesondere durch Eingliederung in Ausbildung oder Arbeit und Sicherung des Lebensunterhalts (§ 1 Abs. 3 Zweites Buch SGB). Zur Erfüllung dieser Aufgaben ist die Kenntnis der Telefonnummer und E-Mail-Adresse der antragstellenden und leistungsbeziehenden Personen nicht erforderlich. Eine postalische Erreichbarkeit ist hierfür ausreichend. Die Erhebung dieser Daten kann daher nur auf freiwilliger Basis erfolgen. Soweit diese Daten nicht be-

reitgestellt werden, dürfen der betroffenen Person hieraus keine Nachteile entstehen.

Die LDI NRW hat das kommunale Jobcenter darauf hingewiesen, dass es sich insoweit nicht datenschutzkonform verhält. Das Jobcenter hat daraufhin die Online-Antragsformulare überarbeitet, so dass die Angabe von Telefonnummer und E-Mail-Adresse wieder auf freiwilliger Basis erfolgen kann.

Fazit

Auch wenn die Erhebung von Daten wie Telefonnummer und E-Mail-Adresse der Antragstellenden nützlich erscheint, ist sie für die Aufgabenerfüllung der Jobcenter nicht zwingend erforderlich. Deshalb dürfen diese Daten nur auf freiwilliger Basis erhoben werden. Aus der Verweigerung der Angabe dürfen den Betroffenen keine Nachteile entstehen.

10. Wirtschaft



10.1. Neue Leitlinien: Europäische Aufsichtsbehörden erläutern wichtige Rechtsgrundlage für Datenverarbeitung durch Unternehmen

Wer personenbezogene Daten anderer verarbeiten will, kann dafür ein eigenes oder fremdes „berechtigtes Interesse" ins Spiel bringen. So sieht es eine Vorschrift vor, die eine der praktisch bedeutsamsten Rechtsgrundlagen im Datenschutzrecht ist, insbesondere für Wirtschaftsunternehmen. Die Vorschrift ist aber oft schwierig in der Anwendung. Neue Leitlinien des Europäischen Datenschutzausschusses schaffen hier mehr Klarheit.

Seit Jahren bereitet dieser Satz Probleme. Zu finden ist er in der DS-GVO, in Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f. Dort heißt es: Die Verarbeitung personenbezogener Daten sei zulässig, wenn diese erforderlich sei „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten", „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

Eine Formulierung, die mehrere unbestimmte Rechtsbegriffe enthält und damit große Interpretationsspielräume eröffnet. So wird bei ihrer Lektüre nicht unmittelbar klar, welches die berechtigten Interessen sind, für die Verantwortliche wie etwa Wirtschaftsunternehmen die personenbezogenen Daten anderer verarbeiten dürfen. Und es bleibt vage, wann genau diese angeführten berechtigten Interessen so stark sind, dass sie Grundrechte oder Grundfreiheiten der betroffenen Personen überwiegen – mit der Folge, dass die Verarbeitung ihrer Daten zulässig wäre.

Immer wieder machte deshalb die Anwendung dieser wichtigen Rechtsgrundlage für die Datenverarbeitung Schwierigkeiten und führte zu Unsicherheit bei Datenverarbeitern wie Betroffenen. Diese Situation hat der EDSA nun zu einem großen Teil bereinigt. In neuen Leitlinien, die im Oktober 2024 veröffentlicht wurden, erläutert er nicht nur den Begriff des „berechtigten Interesses". Der EDSA gibt den Beteiligten unter anderem auch Abwägungshilfen und beispielhafte Anwendungsfälle an die Hand. Die LDI NRW hat daran intensiv mitgewirkt. Sie stellt die deutsche Ländervertreterin in der Arbeitsgruppe des EDSA, die die Leitlinien erarbeitet hat.

Die Leitlinien nennen nun klare Kriterien für die Bestimmung des Begriffs „berechtigtes Interesse", und zwar „rechtmäßig", „klar und präzise" sowie „real und gegenwärtig". Darüber hinaus veranschaulichen die Leitlinien diese Kriterien mit Beispielen, und erklären, wann welche Interessen Dritter relevant sind.

Da die Datenverarbeitung auch für die Wahrung des geltend gemachten berechtigten Interesses erforderlich sein muss, erläutern die Leitlinien sodann, welcher Maßstab hierbei anzulegen ist. Von besonderer Bedeutung für die praktische Anwendung ist zudem die Abwägung zwischen den berechtigten Interessen des Verantwortlichen und den Interessen der von der Verarbeitung betroffenen Person. Die Leitlinien erörtern hierfür detailliert die Methode, nach der die Abwägung durchzuführen ist. Sie stellen eine Liste der Aspekte auf, die in die Abwägung einzustellen sind.

Dies sind

- die Interessen, Grundrechte und Freiheiten der betroffenen Personen,
- die Auswirkungen der Verarbeitung auf die betroffenen Personen, einschließlich
  - der Art der zu verarbeitenden Daten,
  - des Kontexts der Verarbeitung und
  - aller weiteren Folgen der Verarbeitung,die berechtigten Erwartungen der betroffenen Personen,
- die abschließende Abwägung der gegensätzlichen Rechte und Interessen, einschließlich der Möglichkeit weiterer mildernder Maßnahmen.

Zu jedem dieser Aspekte geben die Leitlinien genauere Auslegungshinweise.

Berücksichtigt wird auch, dass die Möglichkeiten der betroffenen Personen variieren, ihre Rechte nach der DS-GVO auszuüben, je nach verwendeter Rechtsgrundlage. So stellen die Leitlinien zusätzlich die spezifischen Gesichtspunkte dar, die für die verschiedenen Betroffenenrechte jeweils zu beachten sind, wenn Daten auf Grundlage von Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO verarbeitet werden.

Schließlich greifen die Leitlinien verschiedene besonders relevante oder problematische Anwendungsfelder heraus und geben zum Beispiel Hinweise,

- welche besonderen Aspekte bei der Verarbeitung von Kinderdaten im Hinblick auf die besondere Schutzwürdigkeit von Kindern zu berücksichtigen sind,
- was zur Verhinderung von Betrug und Missbrauch bei der Nutzung von Dienstleistungen zu beachten ist, sowie
- wann die Verarbeitung zu Direktmarketingzwecken auf diese Rechtsgrundlage gestützt werden kann und wann eher eine andere Rechtsgrundlage in Betracht zu ziehen ist.

Zur Evaluation der Leitlinien hat der EDSA zwischen Oktober und November 2024 eine sechswöchige öffentliche Konsultation durchgeführt. Die Auswertung der Rückmeldungen war bei Redaktionsschluss dieses Berichts noch nicht abgeschlossen.

Fazit

Die gemeinsamen Leitlinien der Europäischen Datenschutzaufsichtsbehörden zur Auslegung der Rechtsgrundlage der „berechtigten Interessen" stellen eine wichtige Anwendungshilfe für die Praxis dar. Sie sorgen für mehr Einheitlichkeit bei der Rechtsanwendung in Europa.

10.2. Betrugsbekämpfung in der EU: LDI NRW setzt sich für klare Regeln beim Austausch von Zahlungsdaten ein

Aus nahezu jeder Bewegung auf dem Girokonto können Schlüsse gezogen werden über die Kontoinhaber*in, über Kaufverhalten, Freizeitgestaltung, Reisen, Wohnverhältnisse, Unterhaltsverpflichtungen und nicht zuletzt über die Vermögensverhältnisse. Informationen über den Zahlungsverkehr dürfen deshalb nur unter strengen Voraussetzungen weitergegeben werden, selbst wenn es um Betrugsbekämpfung geht.

Die EU-Kommission hat sich neben vieler anderer Ziele auch den Kampf gegen den Betrug mit Zahlungsverkehrsdaten auf die Fahnen geschrieben. Im Juni 2023 veröffentlichte die Kommission deshalb ein Gesetzespaket, das unter anderem Zahlungsdienstleister die Möglichkeit geben soll, personenbezogene Daten untereinander auszutauschen. Zahlungsdienstleister sind nicht nur Kreditinstitute mit Vollbanklizenz, sondern auch weniger streng regulierte Anbieter*innen. Sie wickeln – insbesondere online – Zahlungen zwischen Verkäufer*innen, Kund*innen und deren Finanzinstituten ab und stellen daher eine alternative Zahlungsmöglichkeit beispielsweise zur Kreditkarte dar.

Die Gesetzesvorschläge sollen, laut EU-Kommission, den Verbraucherschutz und den Wettbewerb im Bereich elektronischer Zahlungen verbessern und den Verbraucher*innen den Zugang zu einer breiteren Palette günstigerer Finanzprodukte und -dienstleistungen ermöglichen. Das Gesetzespaket entwickelt dazu den bestehenden Rechtsrahmen für Zahlungsdienstleister (insbesondere die Zweite Zahlungsdienste-Richtlinie - „PSD2") weiter und schafft einen neuen Rahmen, um den Zugang zu und die Weitergabe von Finanzdaten im Hinblick auf bestimmte Finanzdienstleistungen (FIDA) zu erleichtern. In diesem Zusammenhang soll es Zahlungsdienstleistern auch ermöglicht werden, anderen Anbieter*innen zur Erkennung von möglicherweise betrügerischem Verhalten Zahlungsverkehrsdaten zugänglich zu machen.

Die LDI NRW hält das jedoch für problematisch. So fehlen dem vorgestellten Gesetzespaket etwa Regeln, welche personenbezogenen Daten konkret zur Betrugsprävention ausgetauscht und wozu sie verwendet werden dürfen. Daher setzt sich die LDI NRW dafür ein, auf nationaler Ebene bereits geltende Standards auch in europäischen Gesetzgebungsverfahren Geltung zu verschaffen. Als Vertretung der Bundesländer in der zuständigen Arbeitsgruppe des EDSA hat die LDI NRW deshalb klare Vorgaben für den Datenaustausch unter Zahlungsdienstleistern formuliert. Diese haben mit dazu geführt, dass der EDSA 2024 gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) eine Stellung-

nahme zu den EU-Gesetzesvorschlägen veröffentlicht hat, abrufbar unter www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-22024-financial-data-access-and-payments-package_en.

Die Stellungnahme soll dem Datenschutz bei der Betrugsbekämpfung zu mehr Geltung verhelfen. Die Betrugsprävention wird dabei als ein wichtiges Anliegen anerkannt, da der durch Betrug entstehende Schaden letztlich stets in Form von steigenden Kosten von allen Verbraucher*innen getragen werden muss. Dies darf aber nicht zu einem wahllosen Sammeln von Daten führen, sondern muss auf relevante tatsächliche Hinweise beschränkt bleiben, die nachvollziehbar zur Betrugsprävention notwendig sind. Solche klaren Regelungen für die Errichtung und Nutzung von Betrugsdatenbanken fehlen bislang im Gesetzesvorschlag der EU-Kommission gänzlich.

Die Stellungnahme des EDSA enthält deshalb auch Empfehlungen für zusätzliche Datenschutzgarantien, die auf den Erfahrungen der deutschen Aufsichtsbehörden mit sog. „Fraud Prevention Pools" in der Kreditwirtschaft basieren. Ein „Fraud Prevention Pool" ist eine zentrale Sammlung von Daten zur Betrugsprävention.

In Deutschland existieren dazu detailliert ausgearbeitete Regeln, die Eingriffen in die Datenschutzrechte der Kund*innen klare Grenzen setzen. Dabei funktioniert die Betrugsprävention folgendermaßen: Die Kreditinstitute melden klar definierte Hinweise zu Betrugsversuchen und Auffälligkeiten in Bankgeschäften und insbesondere im Zusammenhang mit Zahlungsverkehr. Die teilnehmenden Institute können Informationen zur Betrugsprävention durch autorisiertes Personal abrufen, wenn zu einer konkreten Person, mit der sie in Geschäftsbeziehung stehen, Daten im Pool gespeichert sind. Die Speicherung vager Verdachtsmomente in den Pool und Abfragen ohne konkreten Anlass sind gleichermaßen nicht zulässig. Die DS-GVO erkennt zwar die Betrugsprävention als ein berechtigtes Interesse der Zahlungsdienstleister als Grundlage für den Datenaustausch an. Jedoch muss sich die Datenverarbeitung im für den Zweck der Betrugsprävention erforderlichen Maß halten.

Daran anknüpfend fordert der EDSA in seiner Stellungnahme unter anderem, dass in dem Gesetzespaket der EU-Kommission ebenfalls definiert wird, welche personenbezogenen Daten zur Betrugsprävention unter Zahlungsdienstleistern ausgetauscht werden dürfen. Die Informationen dürfen zudem nicht für andere Zwecke als zur Betrugsprävention verwendet werden, insbesondere nicht für eine Kreditwürdigkeitsprüfung. Auch sollen feste Speicherfristen für die verarbeiteten Daten festgelegt werden. Der Zugriff auf die Daten darf nur durch besonders geschultes Personal erfolgen. Und die Meldung eines Betrugsverdachtsfalles sollte nicht automatisch zur Ablehnung der Zahlung führen, sondern zunächst zu einer vertieften Kontrolle der Transaktion. Andernfalls könnten auch

unbescholtene Verbraucher*innen durch eine Sperrung ihres Zahlungskontos erhebliche Nachteile erleiden, wenn es sich um eine irrtümliche Meldung handelt.

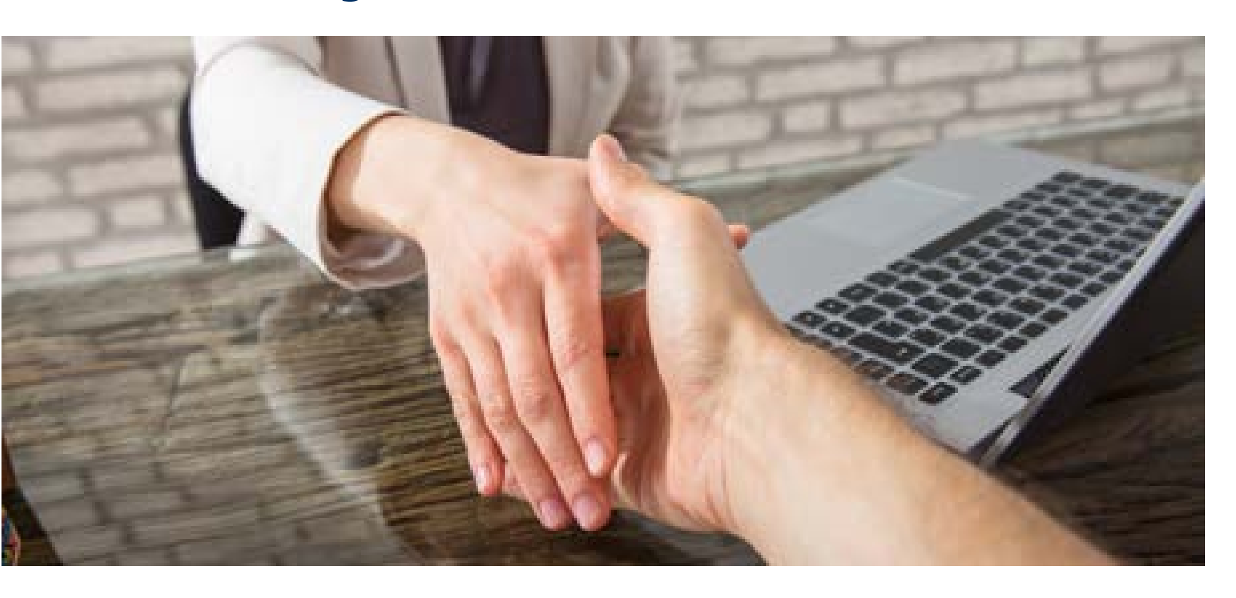
Außerdem äußert sich der EDSA in seiner Stellungnahme zum Zugriff auf personenbezogene Daten von Bankkund*innen durch sog. Zahlungsauslösedienste und Kontoinformationsdienste. Ein Zahlungsauslösedienst ermöglicht die Initiierung einer Zahlung beispielsweise im Online-Shop über ein Zahlungskonto, das bei einem anderen Zahlungsdienstleister geführt wird. Kontoinformationsdienste rufen Kontoinformationen für eine bestimmte Zahl von Tagen in der Vergangenheit ab, etwa Umsätze, Salden und Vormerkposten bei der kontoführenden Bank oder Sparkasse, und bereiten diese für Kund*innen auf.

Hier nimmt der EDSA zu dem Plan Stellung, dass künftig die kontoführenden Zahlungsdienstleister anderen Anbieter*innen den Zugriff auf Kund*innendaten (zum Beispiel auf Zahlungskonten) gewähren sollen, wenn die Einwilligung der Kund*innen jeweils erteilt wurde. Der EDSA weist in diesem Zusammenhang darauf hin, dass dies nur für diejenigen Daten gelten darf, die für die jeweilige Dienstleistung erforderlich sind. Er begrüßt deshalb die Bestrebungen im EU-Parlament, den Umfang der Datenweitergabe einzuschränken. Zum Beispiel sollen Daten vom Geltungsbereich des Vorschlags ausgeschlossen werden, die im Rahmen eines Profilings abgeleitet wurden. Banken dürfen danach beispielsweise das Scoringergebnis der Überprüfung der Kreditwürdigkeit von Kund*innen nicht weitergeben, das sie durch die Schufa erhalten haben.

Fazit

Die Verhinderung von Betrug im Zahlungsverkehr und die Öffnung des Wettbewerbs unter Zahlungsinstituten sind wichtige gesetzgeberische Ziele. Dabei dürfen jedoch die Datenschutzrechte der Kund*innen nicht außer Acht gelassen werden. Ansonsten besteht die Gefahr, dass Betroffene womöglich von Zahlungsdienstleister unberechtigt ausgeschlossen werden und dadurch erhebliche Nachteile im Wirtschaftsverkehr erleiden.

10.3. Unternehmensverkauf per Asset Deal: Neue Orientierungshilfe klärt wichtige Fragen zum Datenschutz



Wer sein Unternehmen verkauft, muss sich auch damit beschäftigen, was mit den Informationen über seine Kund*innen und Beschäftigten passiert. Dürfen sie bei den Erwerbenden landen und, falls ja, wie und wann? Die DSK hat sich erneut mit dem Thema beschäftigt und gibt wichtige Hinweise für den Unternehmensverkauf im Wege des sog. Asset Deals. Eine wertvolle Hilfe für Unternehmer*innen und Datenschutzbeauftragte ebenso wie für Firmenjurist*innen und beratende Rechtsanwält*innen.

Unternehmensverkäufe sind Teil einer funktionierenden Wirtschaftswelt. Dabei werden sie heutzutage vor allem auf zwei Wegen abgewickelt: per Share Deal oder per Asset Deal. Während die Erwerbenden beim Share Deal Firmenanteile übernehmen, kaufen sie beim Asset Deal konkrete Unternehmensteile, also Wirtschaftsgüter und Vermögenswerte.

Ein Asset Deal liegt zum Beispiel vor, wenn ein*e Einzelunternehmer*in den Betrieb veräußert und ein*e Nachfolger*in dabei die Maschinen, den Kundenstamm sowie die Firmierung übernimmt und den Betrieb fortführt. Auch die bestehenden Arbeitsverhältnisse können auf den*die Käufer*in übergehen. Am Ende des „Ausverkaufs" bleibt oft nur noch die Gesellschaft als leere Hülle übrig.

Wer so vorgeht, sollte sich allerdings nicht nur damit beschäftigen, welche Teile er übernehmen will. Auf ihn kommen auch erhebliche datenschutzrechtliche Herausforderungen zu. Kund*innendaten etwa sind von großer wirtschaftlicher Bedeutung und bestimmen auch den Unternehmenspreis. Nicht selten sollen deshalb nicht nur die Basisdaten wie Namen, Anschrift, Geschlecht übergehen, sondern auch Informationen zu getätigten Be-

stellungen. Aber ist das datenschutzrechtlich erlaubt? Ebenso oft ist die Frage zu klären, ob und wann Daten der Beschäftigten an potentielle Käufer*innen weitergegeben werden dürfen.

Um Unternehmer*innen, aber auch Rechtsberater*innen dafür zu sensibilisieren, hat die DSK 2024 dieses schwierige Thema erneut aufgegriffen und ihre Hinweise in einem Beschluss vom 11. September 2024 festgehalten („Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals"). Er ersetzt einen früheren Beschluss vom 24. Mai 2019.

Insbesondere kleinere Firmen wie Einzelkaufleute, Handwerker*innen oder Personengesellschaften und deren Berater*innen sollten den neuen Beschluss kennen. Sie müssen sich mit datenschutzrechtlichen Fragen zur Übermittlung von Informationen befassen. Bei Kapitalgesellschaften gibt es dagegen keine Datenübermittlung, wenn beim Share Deal nur Unternehmensanteile verkauft werden.

In der aktuellen Orientierungshilfe gibt die DSK den Akteur*innen wertvolle Hinweise an die Hand. Verbraucher*innen und Beschäftigte können aus den Hinweisen erkennen, was sie von dem zum Verkauf stehenden Unternehmen erwarten dürfen. Unternehmer*innen, Datenschutzbeauftragte oder Rechtsanwält*innen erfahren, welche Verpflichtungen beim Asset Deal aus dem Datenschutz erwachsen.

So behandelt der Beschluss sowohl den vorvertraglichen Bereich eines Unternehmenskaufs als auch den Umgang mit Kund*innendaten bei Vertragsanbahnung. Er nimmt Stellung zu laufenden und beendeten Verträgen, zu Werbung, Bank- und Beschäftigtendaten. Auch Kleinst- und Kleinunternehmen – also etwa die Handwerksbetriebe – werden in besonderer Weise berücksichtigt.

Im Zentrum des Beschlusses steht zudem das Thema der Einwilligung in den Datenübergang. Meist wollen Unternehmen den Aufwand vermeiden, eine Einwilligung bei jeder einzelnen Person einzuholen. Sie versuchen deshalb, die Datenübermittlung etwa unter Hinweis auf die gesetzliche Norm des Art. 6 Abs. 1 Satz 1 Buchstabe f der DS-GVO zu rechtfertigen. Diese Vorschrift kann in Betracht kommen, wenn ein berechtigtes Interesse an der Datenverarbeitung besteht. Die konkrete Verarbeitung muss aber auch für die Verfolgung dieses Interesses erforderlich sein und es darf keine überwiegenden entgegenstehenden Interessen der Betroffenen geben.

Im Ergebnis billigt der DSK-Beschluss nur in seltenen Fällen die Verarbeitung gemäß Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO. In der Mehrzahl der verschiedenen Fallkonstellationen bedarf es einer informierten, freiwilligen und unmissverständlichen Zustimmung der Betroffenen vor dem Datentransfer.

Eine Ausnahme sieht die DSK bei Kleinst- und Kleinunternehmen, wenn diese die Kund*innendaten einem anderen Klein- oder Kleinstunternehmen desselben Wirtschaftszweiges übergeben. Hier ist – gestützt auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO – die einmalige Übermittlung der Postadressen im Wege einer Widerspruchslösung erlaubt.

Widerspruchslösung bedeutet in diesem Falle, dass die Kund*innen über die bevorstehende Unternehmensveräußerung unterrichtet werden und innerhalb einer angemessenen Frist von ca. vier bis sechs Wochen formlos dem Datentransfer widersprechen können. Die Erwartungen und Interessen der Kund*innen werden so berücksichtigt.

Wie sehr es dabei auf die Feinheiten ankommt, zeigt sich aber auch hier: Die Erlaubnis zum Einsatz der Widerspruchslösung betrifft nur die Postadresse. Für die Übermittlung von Telefonnummern und E-Mail-Adressen bedarf es weiterhin der vorherigen Einwilligung der Betroffenen.

Der Beschluss wurde vom Arbeitskreis Wirtschaft der DSK vorbereitet, den die LDI NRW leitet.

Fazit

Mit den erneuerten Hinweisen zum Asset Deal schafft die DSK eine wichtige Orientierungshilfe für Verbraucher*innen und Firmeninhaber*innen beim Unternehmensverkauf – unter besonderer Berücksichtigung der Situation von Kleinst- und Kleinunternehmen. Rechtsberatende Institutionen wie Verbänden und Wirtschaftsorganisationen erhalten zudem eine gute Basis, auf die sie ihre Beratung bei Unternehmensnachfolgen aufbauen können.

10.4. Wirtschaftsauskunfteien erhalten neue Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten

Die deutschen Wirtschaftsauskunfteien haben sich in Absprache mit der Datenschutzaufsicht vor Jahren selbst Verhaltensregeln gegeben. Diese sind nun überarbeitet worden, nicht zuletzt angestoßen durch neue Rechtsprechung des Europäischen Gerichtshofs. So dürfen etwa viele Daten nicht mehr so lange gespeichert werden.

Wirtschaftsauskunfteien sind aus dem Leben der Deutschen nicht mehr wegzudenken. Ob es um eine Kreditaufnahme geht oder schlicht das Mieten einer Wohnung – immer mehr Auftraggeber greifen auf Daten über die Kreditwürdigkeit und Zahlungsfähigkeit von Unternehmen und Privatpersonen zurück, die von den Wirtschaftsauskunfteien gesammelt und verkauft werden. Zu den bekanntesten Vertretern dieser Branche zählen etwa die SCHUFA und Creditreform.

Dabei greifen die Auskunfteien regelmäßig auch auf personenbezogene Daten zurück, was klare datenschutzrechtliche Regelungen für dieses Vorgehen verlangt – vor allem in Bezug auf die Speicherung und Löschung dieser Informationen. Mit dem Code of Conduct (CoC), den sich die Branche in Absprache mit den Datenschutzaufsichtsbehörden gegeben hat, präzisiert der Verband die gesetzlichen Regelungen zur Speicherdauer und Löschung für die Auskunfteien. Nun ist dieser selbst gewählte Verhaltenskodex – unter Beteiligung der LDI NRW – erheblich erneuert worden.

Konkret geht es um den CoC für die Prüf- und Löschfristen der Wirtschaftsauskunfteien aus dem Jahr 2018/2020. Dessen Regeln sind mit dem 25. Mai 2024 von neuen Verhaltensregeln abgelöst worden. Nach zahlreichen Beratungen des Verbandes „Die Wirtschaftsauskunfteien e.V" mit den deutschen Datenschutzaufsichtsbehörden hat der örtlich zuständige Hessische Beauftragte für Datenschutz und Informationsfreiheit die neuen Verhaltensregeln mit zahlreichen Verbesserungen in datenschutzrechtlicher Hinsicht genehmigt. An diesen Beratungen waren neben der LDI NRW auch die Aufsichtsbehörden aus Bayern (LDA BY) und Baden-Württemberg beteiligt. Ursprünglich war die LDI NRW für den CoC zuständig, die Aufsicht war auf Hessen übergegangen, weil der Verband nach Wiesbaden umgezogen ist.

Ende 2023/Anfang 2024 gab es zwei wesentliche Gründe, weshalb der CoC einer Prüfung unterzogen werden musste. Zum einen bestand eine Pflicht des Verbandes, das Regelwerk zu überprüfen und die Aufsichtsbehörden daran zu beteiligen. Zum anderen gab es neue Rechtsprechung des Europäischen Gerichtshofs zur Speicherdauer, und zwar konkret bezogen

auf das Merkmal „Restschuldbefreiung" im Datenbestand der Auskunfteien. Unter Restschuldbefreiung ist die Möglichkeit zu verstehen, dass sich ein Schuldner nach einigen Jahren von Schulden befreien lassen kann, die von diesem nicht bezahlt werden können. Laut EuGH dürfen dieses Merkmal und alle damit im Kontext stehenden Informationen – orientiert am amtlichen Insolvenzregister – nur sechs Monate gespeichert werden. Danach ist die Information im Datenbestand zu löschen. Bislang war eine Speicherdauer von drei Jahren vorgesehen.

Die darauf aufsetzende Überarbeitung des CoC bringt nun klare Verbesserungen für den Datenschutz. So ist der CoC insgesamt strukturierter geworden. Das zeigt sich vor allem durch ein Begriffsglossar zu Beginn und durch die Nennung von Rechtsvorschriften, durch die die Datennutzung in ihrem Zweck begrenzt wird. Der CoC regelt allerdings generell nicht, ob die Verarbeitung der Daten rechtmäßig ist, sondern konkretisiert nur die berechtigte Speicherdauer. Eine neutrale Überprüfung kann über die jeweilige Überwachungsstelle erreicht werden, die in den Kontaktdaten des CoC aufgeführt ist.

Neu ist außerdem, dass es bei nicht ausgeglichenen Forderungen zwar bei dem dreijährigen Speicherzeitraum verbleibt, er aber bei ausgeglichenen Forderungen auf die Hälfte reduziert werden muss, wenn bestimmte Voraussetzungen vorliegen. Die Speicherung von Daten aus amtlichen Schuldnerverzeichnissen und Insolvenzbekanntmachungen dürfen nicht länger als drei Jahre gespeichert werden, sondern richten sich nach der Speicherdauer in dieser jeweiligen amtlichen Veröffentlichung. Das macht sich vor allem bei der Restschuldbefreiung und den von ihr umfassten Forderungen bemerkbar, die nur noch sechs Monate lang gespeichert werden dürfen.

Eine starke Beschränkung erfolgt auch hinsichtlich der Speicherung von Positivdaten – also von störungsfrei laufenden Verträgen. Diese dürfen nur noch zur Prüfung der Kreditwürdigkeit und im Zusammenhang mit Bankgeschäften für drei Jahre gespeichert werden. Für Energielieferverträge oder Mobilfunkverträge ist das nun nicht mehr möglich. Auch Daten von früheren Anschriften sowie Betrugsverdachtsinformationen sind nur in begrenztem Maße speicherbar.

Eine weitere wesentliche Verbesserung durch mehr Transparenz wird durch den neuen Abschnitt zur neutralen Überwachungsstelle erreicht, die von der LDI NRW akkreditiert worden ist. Hier werden das Aufgabenspektrum und die Einzelheiten des Beschwerdeverfahrens dargestellt. Damit steht Betroffenen ein spezielles Beschwerdeverfahren zur Verfügung, das effizient und direkt zur Klärung eines Problems mit den Auskunfteien genutzt werden kann. Neben diesem Beschwerdeverfahren bleibt selbstverständlich eine Beschwerde bei der LDI NRW als Aufsichtsbehörde weiterhin möglich.

Fazit

Durch den Einsatz der Datenschutzaufsichten konnte erreicht werden, dass die zentralen Verhaltensregeln für Wirtschaftsauskunfteien aus datenschutzrechtlicher Sicht verbessert wurden. Einige Möglichkeiten der Auskunfteien zur Speicherung von Daten wurden gänzlich gestrichen, teilweise wurden Fristen verkürzt. Außerdem wurden Verwendungszwecke präzisiert und viele Regelungen transparenter gestaltet.

10.5. LDI NRW bringt Datenschutz-Zertifizierung in Deutschland weiter voran – Angebot wird erweitert



In Deutschland gibt es jetzt einen zusätzlichen Kriterienkatalog, nach dem Unternehmen ein Datenschutz-Zertifikat erhalten können. Die LDI NRW hat 2024 den entsprechenden Katalog des Forschungsprojekts „Auditor" genehmigt, der sich speziell an Anbieter*innen von Cloud-Diensten richtet. Damit baut Deutschland seine europäische Vorreiterrolle in der Datenschutz-Zertifizierung aus.

Wie lässt sich Datenschutz in Deutschland transparenter und verlässlicher machen? Eine wesentliche Rolle spielt dabei die Zertifizierung von Datenverarbeitungsvorgängen. Unternehmen können mit einem Zertifikat belegen, dass ihre Angebote datenschutzkonform sind – und dass dies von einer unabhängigen Zertifizierungsstelle anhand eines geneh-

migten Kriterienkatalogs bestätigt wurde. Wer einen Auftragsverarbeiter beauftragen will, dem kann wiederum ein Zertifikat bei der Auswahl geeigneter Dienstleister*innen helfen.

Schon früh hat die LDI NRW daran mitgewirkt, dass ein solches Zertifizierungssystem in Deutschland Einzug hält – indem Zertifizierungsstellen geschaffen und Kriterienkataloge entwickelt und zugelassen werden, die als Grundlage für die Arbeit der Zertifizierungsstellen dienen. Ende 2022 genehmigte die LDI NRW den ersten dieser Kataloge in Deutschland, im Dezember 2023 wurde mit der EuroPriSE Cert GmbH die erste deutsche Zertifizierungsstelle zugelassen.

2024 hat die LDI NRW nun einen weiteren Kriterienkatalog genehmigt. Vorausgegangen war, dass der EDSA die Genehmigungsfähigkeit des Projekts festgestellt hatte (Stellungnahme 7/2024 vom 17. April 2024). Der neue Kriterienkatalog des Forschungsprojekts „Auditor" richtet sich speziell an Anbieter*innen von Cloud-Diensten des privaten Sektors, welche ihre Dienstleistung für Unternehmen oder Privatpersonen erbringen. Dabei ist der Kriterienkatalog Teil eines umfassenden Programms, das die Datenschutzkonformität der jeweiligen Angebote bewertet. Das Programm definiert detaillierte Kriterien und Methoden für die Begutachtung von Cloud-Diensten und berücksichtigt dabei die spezifischen Gegebenheiten solcher Dienste.

Die LDI NRW hatte das „Auditor"-Projekt anhand der übermittelten Unterlagen auf die Vereinbarung mit europäischem Datenschutzrecht zu überprüfen. Stellungnahmen von weiteren Datenschutzaufsichtsbehörden wurden dazu eingeholt und deren Änderungsanforderungen koordiniert.

In dem Verfahren hat die LDI NRW darauf hingewirkt, dass die Zertifizierung auch für Privatpersonen wirkt, soweit ihre Datenverarbeitung unter die sog. Haushaltsausnahme fällt. Im Rahmen der Haushaltsausnahme finden die Datenschutzregeln der DS-GVO ausnahmsweise keine Anwendung, sofern personenbezogene Daten durch eine Privatperson verarbeitet werden und dies ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten erfolgt. Gerade solche persönlichen und familiären Datenverarbeitungen aber benötigen besonderen Schutz. Durch die Auswahl eines zertifizierten Cloud-Dienstes können sich nun zukünftig auch Privatpersonen über die Seriosität der Dienstleistung anhand von Zertifikaten vergewissern.

Dass eine nicht der DS-GVO unterfallende Datenverarbeitung dennoch in den Wirkungskreis der DS-GVO-Zertifizierung einbezogen werden kann, war allerdings diskussionsbedürftig. Nach intensiven Beratungen auf europäischer Ebene konnte sich die von der LDI NRW vertretene Auffassung durchsetzen, wonach Cloud-Dienstleister*innen auch

in einem solchen Fall an die DS-GVO gebunden sind – und die Haushaltsausnahme damit kein Hindernis für eine Zertifizierung der Cloud-Dienstleister*innen nach den „Auditor"-Vorgaben darstellt.

Die Folgen daraus sind erheblich: Im Ergebnis kann ein so erteiltes Zertifikat künftig den gesamten Kundenkreis ansprechen. Es bietet somit für Cloud-Anbieter*innen einen erhöhten Mehrwert in der Außenwirkung.

Mit der abgeschlossenen Genehmigung des Kriterienkatalogs von „Auditor" können sich interessierte Unternehmen nun auf Basis des darin enthaltenen Konformitätsbewertungsprogramms als Zertifizierungsstelle bei der Deutschen Akkreditierungsstelle akkreditieren. Diese prüft, ob Antragstellende die Kompetenz besitzen, entsprechende Zertifizierungsverfahren durchzuführen.

Fazit

Mit der Genehmigung des „Auditor"-Kriterienkatalogs bringt die LDI NRW die Entwicklung umfassender und transparenter Datenschutzpraktiken weiter voran. Sie stärkt zugleich Deutschlands Rolle als europäischer Vorreiter in der Datenschutz-Zertifizierung.

10.6. Wirtschaftsauskunfteien: Beim Scoring muss weiter kontrolliert werden

Berücksichtigen die Wirtschaftsauskunfteien in NRW die aktuelle Rechtsprechung des Europäischen Gerichtshofs zur Speicherdauer von Daten zur Restschuldbefreiung und zum Umgang mit dem Scoring? In einem Punkt jedenfalls gibt es Zweifel.

Wirtschaftsauskunfteien sammeln Daten über Unternehmen und Menschen, und diese Daten sind oft heikel. Außerdem bewerten sie diese Daten, indem sie etwa die Zahlungsfähigkeit oder Kreditwürdigkeit analysieren. So speichern sie zum Beispiel, ob für eine Person eine sog. Restschuldbefreiung gilt, die Person sich also nach einigen Jahren von Schulden befreien lassen kann. Die Auskunfteien arbeiten außerdem mit dem sog. Scoring. Das Verfahren dient zur Ermittlung der Bonität von Verbraucher*innen oder Unternehmen, die später als Note in einer Ratingskala dargestellt wird.

Welche Regeln aber gelten für diese erheblichen Eingriffe aus datenschutzrechtlicher Sicht? Der EuGH hat in den Rechtssachen C-634/21 (SCHUFA Holding/Scoring) und C-26/22, C-64/22 (SCHUFA Holding/Restschuldbefreiung) dazu zwei wichtige Entscheidungen getroffen, die sich auf die Datenverarbeitung der Wirtschaftsauskunfteien und ihrer Unternehmenskund*innen auswirken: Zum einen darf eine Auskunftei das Datum der Restschuldbefreiung im Datenbestand nicht länger als nach dem Registerrecht zulässig – also 6 Monate – speichern und verarbeiten. Zum anderen ist das Scoring eine laut Art. 22 DS-GVO verbotene automatisierte Entscheidung im Einzelfall, sofern die Auskunfteikund*innen dem übermittelten Score eine „maßgebliche Rolle" im Rahmen ihrer Vertragsentscheidung einräumen.

Dazu muss man wissen, dass die Kund*innen von Auskunfteien unter anderem Online-Händler oder Banken sind, die mit Personen Kaufverträge oder Kreditverträge abschließen. Über die Auskunfteien wollen sie ermitteln, ob ihre Vertragspartner*innen ihren Zahlungsverpflichtungen in der Zukunft werden nachkommen können. So hat für sie eine wichtige Aussagekraft, dass bei einer Person ein Verbraucherinsolvenzverfahren anhängig war und dieses durch Entgegenkommen der Gläubiger*innen und schuldnerisches Wohlverhalten zu einer Befreiung von der Restschuld geführt hat. Das Scoring, ein mathematisch-statistisches Verfahren, ermöglicht ihnen zudem, die Wahrscheinlichkeit eines künftigen Verhaltens statistisch einzuschätzen, etwa die Rückzahlung eines Kredits.

Für die betroffenen Personen und Unternehmen haben die Speicherung dieser Daten und die Auskunftserteilung zu diesen Informationen eine wichtige Bedeutung, weil sie den Abschluss von Verträgen beeinflussen. Die LDI NRW hat deshalb die EuGH-Entscheidungen zum Anlass genommen, die Wirtschaftsauskunfteien, die ihren Sitz in NRW haben, dazu zu befragen, ob sie die Gerichtsentscheidungen umsetzen und wie. Konkret wurden die Unternehmen gefragt:

1. *Haben Sie in Ihrem Datenbestand Daten zur Restschuldbefreiung, die älter als 6 Monate sind, gelöscht und Ihre Löschroutine angepasst? Haben Sie dabei auch sämtliche sonstige Forderungsdaten gelöscht, die zur Insolvenz geführt haben und mit der Restschuldbefreiung abgeschlossenen worden sind?*

   Hierzu haben die Auskunfteien angegeben, dass sie das Klageverfahren vor dem EuGH beobachtet hätten und bereits im Vorfeld in Erwartung der nun vorliegenden Entscheidung ihre Löschroutine an diese Sechsmonatsfrist des amtlichen Insolvenzregisters angepasst und bereits ältere Daten gelöscht hätten – einschließlich sämtlicher sonstigen Forderungsdaten, die zur Insolvenz geführt haben und mit der Restschuldbefreiung abgeschlossen worden seien. Für die LDI NRW gab es insofern nichts zu beanstanden.

2. *Wie stellen Sie sicher, dass der von Ihnen übermittelte Score zu einer Person keine maßgebliche Rolle für die vertraglichen Entscheidungen der Datenempfänger*innen einnimmt. Falls dies nicht sichergestellt werden kann, legen Sie bitte dar, wie die Anforderungen des Art. 22 DS-GVO gewahrt werden. Ich bitte Sie um anonymisierte Darstellung der Prozesse bei Ihren Datenempfänger*innen, die dieses Maßgeblichkeitskriterium berücksichtigen (Best Practices). Die Anforderung weiterer Nachweise bleibt vorbehalten.*

   Zu diesen Fragen haben die Auskunfteien ausgeführt, dass die Scorenutzer*innen (zum Beispiel Onlinehändler, Versandhändler), denen die Auskunfteien Scorewerte übermitteln, diese Scorewerte keineswegs zu ihrem alleinigen Entscheidungskriterium gemacht hätten. Vielmehr flössen neben dem Score noch weitere Kriterien ein wie eigene Zahlungserfahrungen bei Bestandskund*innen, sonstige offene Forderungen, Guthaben, Warenkorbhöhe. Diese Aussage wird die LDI NRW mit weiteren Kontrollmaßnahmen überprüfen müssen. Dazu werden sich die Datenschutzaufsichtsbehörden auch darauf verständigen müssen, unter welchen Umständen ein Score nicht mehr maßgeblich für die Entscheidung ist, der er zugrunde gelegt wurde. Die Abstimmung unter den Aufsichten läuft derzeit in den Fachgremien der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder.

Fazit

Die Orientierung der Speicherfrist für die Restschuldbefreiung in Wirtschaftsdatenbanken an der Speicherfrist im amtlichen Register ist mit den Urteilen des EuGH erreicht und wird von den Auskunfteien offenbar beachtet. Die Frage, ob ein Scorewert maßgeblich für eine vertragliche Entscheidung ist, muss weiter geklärt werden und dann bei den Scorenutzer*innen in den verschiedenen Wirtschaftsbereichen überprüft werden.

10.7. Betrugsprävention ja – aber bitte datenschutzkonform! LDI NRW geht gegen Austausch von Gesundheitsdaten vor

Versicherungskonzerne in zehn Bundesländern und dem europäischen Ausland haben über einen geschlossenen E-Mail-Verteiler rechtswidrig Daten von Kund*innen in der Auslandsreisekrankenversicherung geteilt. Die LDI NRW hat daraufhin eine gemeinsame koordinierte Prüfung mit anderen Aufsichtsbehörden angeregt und in Angriff genommen.

Der Zweck muss stets die Mittel heiligen. Diese goldene Regel haben offenbar knapp 40 Unternehmen aus der Versicherungsbranche aus dem In- und Ausland gründlich missverstanden. Man kam dort auf die Idee, möglichen Betrugsfällen in der Auslandsreisekrankenversicherung nachzuspüren und Betrugsmuster zu identifizieren – und dazu Kund*innendaten auszutauschen. Doch weder gab es für den Austausch eine Rechtsgrundlage noch trafen die Unternehmen Vorkehrungen zum Schutz der Kund*innendaten. Da elf der Unternehmen in NRW ansässig sind, hat die LDI NRW als die zuständige Aufsichtsbehörde 2024 eine Überprüfung dieser Unternehmen eingeleitet.

Konkret erfolgte der Austausch der Daten zu potentiellen Betrugsfällen über einen geschlossenen E-Mail-Verteiler, auf dem meist mehrere Beschäftigte der beteiligten Unternehmen registriert waren. Betroffen waren fast ausschließlich Versicherungsfälle in der Auslandsreisekrankenversicherung. Dabei wurden auch sensible Gesundheitsdaten wie etwa medizinische Diagnosen sowie Daten minderjähriger Personen ausgetauscht, ohne Vorkehrungen zum Schutz personenbezogener Daten oder zur Wahrung der Betroffenenrechte vorzusehen. Jedes der knapp 40 Unternehmen, das an dem Verteiler beteiligt war, erhielt umfangreiche Informationen zu vermeintlichen Betrugsverdachtsfällen. Und das auch, wenn die von dem Datenaustausch Betroffenen in keinerlei Kontakt zu dem jeweiligen Unternehmen standen und es somit keinen Grund gab, das Unternehmen über einen bestehenden Betrugsverdacht zu unterrichten.

Für eine solche Vorgehensweise fehlt es erkennbar an einer Rechtsgrundlage. Zwar ist die Betrugsprävention ein berechtigtes Interesse im Sinne der DS-GVO, so dass die Verarbeitung personenbezogener Daten grundsätzlich hätte zulässig sein können. In der Art und Weise aber, wie der Datenaustausch erfolgte, war er nach den derzeitigen Erkenntnissen rechtswidrig.

Die Nutzung dieses Systems erstaunt umso mehr, als es eine mit den Datenschutzaufsichtsbehörden abgestimmte, seit Jahren im Versicherungssektor etablierte Möglichkeit des datenschutzkonformen Austauschs über potentielle Betrugsfälle für bestimmte Versicherungsprodukte

gibt. Dieses „HIS" genannte System kennt klar geregelte Kriterien für Ein- und Ausmeldungen, sichert Betroffenenrechte und sieht Löschfristen vor. Insbesondere erlaubt es nicht, dass Daten ohne Bezug zu einem bestehenden oder sich anbahnenden Vertragsverhältnis oder einem Leistungsantrag abgefragt werden. Auch ist eindeutig geregelt, welche personenbezogenen Daten verarbeitet werden dürfen – die Auslandsreisekrankenversicherung wie auch andere Versicherungsprodukte mit Gesundheitsdaten gehören allerdings gerade nicht dazu. Denn über das HIS werden keine Gesundheitsdaten ausgetauscht. Es ist daher möglich, dass die Unternehmen den illegalen Weg über den E-Mail-Verteiler genutzt haben, um sich neben den Betrugsverdachtsfällen in der Auslandsreisekrankenversicherung auch über entsprechende Gesundheitsdaten austauschen zu können.

Die LDI NRW hat als erste Aufsichtsbehörde von der illegalen Praxis erfahren und daraufhin eine enge Kooperation mit den anderen zuständigen Datenschutzaufsichtsbehörden im In- und Ausland angestoßen. Dies führte zu einem koordinierten und zeitgleichen Vorgehen der beteiligten Aufsichtsbehörden gegenüber den betroffenen Unternehmen. Gegenüber den elf teilnehmenden Unternehmen aus NRW wurden bereits erste Maßnahmen getroffen und der rechtswidrige Austausch abgestellt. Auch müssen die Unternehmen die betroffenen Kund*innen über die rechtswidrige Datenverarbeitung informieren, damit diese ihre Rechte wahrnehmen können.

Im nächsten Bericht der LDI NRW soll über den Fort- bzw. Ausgang dieses Verfahrens berichtet werden.

Fazit

Die Aufdeckung von Versicherungsbetrug nützt der gesamten Versichertengemeinschaft, die andernfalls die durch Betrugsfälle entstandenen Kosten in Form erhöhter Prämien zu tragen hat. Wenn jedoch die Mittel zur Erreichung dieses Zwecks rechtswidrig sind, kann die Rechtsordnung übermäßiger Eingriffe in die Privatsphäre nicht hinnehmen. Der Versicherungsbranche kann nur geraten werden, vor dem Installieren von Systemen zur Betrugserkennung den Dialog mit den Aufsichtsbehörden zu suchen.

11. Werbung



11.1. Pur-Abo-Modelle machen Schule – Datenschutzbehörden stellen Regeln auf

Viele Medienhäuser arbeiten mittlerweile auf ihren Websites mit Modellen, die Informationen gegen Daten anbieten. Nach den deutschen Aufsichtsbehörden hat sich nun auch der EDSA mit der Rechtmäßigkeit solcher Pur-Abo-Modelle beschäftigt. Allerdings hat er vorerst nur Regeln für die großen Online-Plattformen aufgestellt.

Leser*innen von Online-Zeitungen kennen sie meist – die sog. Pur-Abo-Modelle. Gemeint sind Websites, die Nutzer*innen erst aufrufen können, wenn sie einen zahlungspflichtigen Abo-Vertrag abgeschlossen oder ihre Zustimmung zum Tracking ihrer Nutzerdaten erteilt haben. Immer mehr Medienhäuser, aber auch Websites aus anderen Bereichen entscheiden sich für eine derartige Gestaltung.

Die LDI NRW hat sich schon 2023 damit beschäftigt, ob solche Modelle datenschutzkonform sind. Siehe 29. Bericht unter 7.4. anlässlich eines Beschlusses der DSK zu Pur-Abo-Modellen hat die LDI NRW festgehalten, dass deren Einsatz zwar grundsätzlich zulässig sein kann. Jedoch müssten hierbei alle Voraussetzungen der DS-GVO eingehalten werden. Insbesondere müssten Nutzer*innen die Möglichkeit haben, zu einzelnen Zwecken oder zu Bündeln zusammenhängender Zwecke einzuwilligen.

Nun hat 2024 das Thema auch die europäische Ebene erreicht. Der EDSA nennt erstmals klare Voraussetzungen dafür, wann große Online-Plattformen derartige Pur-Abo-Modelle einsetzen können.

Am 17. April 2024 hat der EDSA seine Stellungnahme „Wirksame Einwilligung im Kontext von Pur-Abo-Modellen, die von großen Online-Plattformen umgesetzt werden” veröffentlicht, abrufbar unter www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en. Unter „großen Online-Plattformen” versteht der EDSA soziale Plattformen mit einer großen Anzahl von Nutzern, einer gewissen Marktmacht und einer großen verarbeiteten Datenmenge. Sehr große Plattformen und Gatekeeper. wie beispielsweise Meta und Google, fallen in jedem Fall unter diese Definition. Aber auch nicht ganz so große Online-Plattformen sind von der Stellungnahme des EDSA erfasst.

Unter bestimmten Voraussetzungen kann das Pur-Abo-Modell für große Online-Plattformen auch nach Auffassung des EDSA rechtmäßig sein. Dies ist zum Beispiel dann der Fall, wenn beim Pur-Abo-Modell sämtliche Anforderungen der DS-GVO, insbesondere jene an eine wirksame Einwilligung, erfüllt werden. Die Anforderungen, die der EDSA an große Online-Plattformen stellt, gehen über die im DSK-Beschluss benannten Voraussetzungen hinaus.

Der EDSA stellt in seiner Stellungnahme insbesondere klar, dass es großen Online-Plattformen in den meisten Fällen nicht möglich sein wird, die Anforderungen an eine wirksame Einwilligung zu erfüllen, wenn sie Nutzer*innen nur zwischen zwei Optionen wählen lassen: einerseits die Einwilligung in die Verarbeitung personenbezogener Daten für Zwecke der verhaltensorientierten Werbung und andererseits in die Zahlung eines Entgelts. Daraus zieht der EDSA die Schlussfolgerung, dass es nicht der Standardweg für Plattformanbieter sein sollte, Nutzer*innen vor die Alternative zu stellen, den Dienst unter Hinnahme von Tracking zu Werbezwecken zu nutzen oder ein mit teilweise hohen Kosten verbundenes Pur-Abo abzuschließen. Vielmehr sollten die Plattformanbieter nach Ansicht des EDSA in Erwägung ziehen, den betroffenen Personen eine „gleichwertige Variante” anzubieten, für die keine Gebühr zu entrichten ist, gleichzeitig aber auch keine oder weniger Nutzerdaten zum Zwecke der verhaltensbezogenen Werbung verarbeitet werden.

Eine weitere wichtige Bedingung für das Vorliegen einer freiwilligen Einwilligung ist auch nach Auffassung des EDSA die Granularität: Wenn der betroffenen Person ein Pur-Abo-Modell präsentiert wird, sollte es ihr freistehen, (nur) die von ihr akzeptierten Verarbeitungszwecke zu wählen. Dagegen ist es unzulässig, mit einem einzigen Einwilligungsersuchen sämtliche Zwecke zusammenzufassen, ohne Nutzer*innen eine Wahl zu eröffnen. Bei Pur-Abo-Modellen großer Online-Plattformen ist es nach Auffassung des EDSA zudem besonders wichtig, dass Nutzer*innen keinen irreführenden Gestaltungsmustern ausgesetzt werden. Das heißt, dass die Einwilligungsbanner so gestaltet sein müssen, dass für die Nutzer*innen leicht erkennbar ist, welche Handlung sie durch welchen Klick vornehmen.

Damit die Einwilligung „in Kenntnis der Sachlage" erfolgt, muss der Plattformanbieter ausweislich der EDSA-Stellungnahme die Nutzer*innen transparent und vollständig darüber informieren, welche Folgen die Einwilligungen für die Verarbeitung der Nutzer*innendaten haben können. Dies stellt oft eine große Herausforderung für die Anbieter*innen dar, zumal die Verarbeitungen der Nutzer*innendaten im Zusammenhang mit verhaltensorientierter Werbung meist sehr umfangreich und komplex sind.

Darüber hinaus betont der EDSA, dass Betroffene nicht benachteiligt werden dürfen, wenn sie weder in das Werbe-Tracking einwilligen noch ein Pur-Abo abschließen. Vom Vorliegen eines Nachteils geht der EDSA etwa dann aus, wenn der Dienst für die Teilhabe am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken eine herausragende oder entscheidende Rolle spielt.

Zudem fließt laut Stellungnahme des EDSA auch die Höhe des Entgelts in die Bewertung ein. Die Betreiber*innen von großen Online-Plattformen müssen daher von Fall zu Fall bewerten, ob ein Entgelt als solches sowie die Höhe selbst angemessen sind.

Der EDSA entwirft derzeit Leitlinien zum Thema „Wirksame Einwilligung im Kontext von Pur-Abo-Modellen", die einen weiteren Anwendungsbereich haben als die Stellungnahme und sich nicht ausschließlich auf große Plattformanbieter*innen, sondern auf alle Websitebetreiber*innen mit Pur-Abo-Modellen beziehen werden. Es steht noch nicht fest, wann die Leitlinien fertiggestellt sind. Die genauen Formulierungen und Auswirkungen auf die Praxis bleiben abzuwarten.

Fazit

Die EDSA-Stellungnahme zum Thema „Wirksame Einwilligung im Kontext von Pur-Abo-Modellen, die von großen Online-Plattformen umgesetzt werden" bezieht sich auf große Online-Plattformen, nicht aber auf andere Websitebetreiber*innen. Sie ergänzt insoweit den Beschluss der DSK und bestätigt die wesentlichen Elemente dieses Beschlusses.

11.2. Welche Verhaltensregeln gelten beim grenzüberschreitenden Direktmarketing per Post?

Werbung funktioniert längst über Grenzen hinweg. Doch gibt es ein einheitliches Verständnis der Regelungen dafür? Die österreichische Datenschutzbehörde hat einen Entwurf für Verhaltensregeln beim postalischen grenzüberschreitenden Direktmarketing vorgelegt – und die deutschen Aufsichtsbehörden gefragt, was sie davon halten. Es gibt noch Klärungsbedarf.

Direktmarketing ist eine Werbemaßnahme, bei der bestehende und potenzielle Kund*innen direkt angesprochen werden. Der Kontakt wird dabei beispielsweise per Hausbesuch, E-Mail oder Telefon hergestellt – oder auch per Briefpost. Die Unternehmen benötigen dafür allerdings persönliche Daten der Angeschriebenen, zumindest deren Adressen. Noch besser funktioniert das Direktmarketing, wenn die Werbetreibenden darüber hinaus Informationen über Vorlieben und Kaufverhalten der möglichen Kund*innen besitzen.

Damit kommt allerdings der Datenschutz ins Spiel und die Frage, ob und wann ein solches Direktmarketing zulässig ist. Und nicht nur das: Im Zeitalter der Globalisierung erfolgt Direktmarketing oft länderübergreifend. Da ist es hilfreich, wenn in den betroffenen Staaten die gleichen Regeln und Auffassungen gelten. 2024 hat die österreichische Datenschutzbehörde die deutschen Aufsichtsbehörden um ihre Meinung zu einem österreichischen Entwurf für Verhaltensregeln beim postalischen grenzüberschreitenden Direktmarketing gebeten. Zielvorstellung sind verbindliche transnationale Verhaltensregeln („Code of Conduct" – CoC), die es österreichischen Unternehmen ermöglichen, postalisches Direktmarketing sowohl im eigenen Land als auch im weiteren deutschsprachigen europäischen Raum datenschutzrechtskonform durchzuführen. Dieser Raum umfasst neben Österreich und Deutschland auch Südtirol in Italien. Solche Verhaltensregeln können von Verbänden vorgelegt werden und die DS-GVO präzisieren. Der Entwurf dieser Verhaltensregeln wurde vom Dialog Marketing Verband Österreich (Antragsteller) und der Federation of European Data and Marketing (Mitinhaber) erarbeitet.

Die LDI NRW wie auch die anderen deutschen Aufsichtsbehörden behandeln viele der im CoC aufgeworfenen Fragestellungen unter dem Begriff des „Adresshandels". Unter Adresshandel verstehen sie dabei sowohl die Erhebung als auch die weitere Verarbeitung personenbezogener Daten, die das Ziel haben, Werbetreibenden Direktwerbung zu ermöglichen. Adresshandel steht mit Direktwerbung in einem engen sachlichen Zusammenhang. Adresshändler*innen bieten Postadressen solchen Unternehmen an, die für ihre Waren und Dienstleistungen wer-

ben und zielgerichtet Personen anschreiben wollen. Sie können aber auch für Unternehmen die Werbung selbst datenschonend durchführen, ohne Adressen an diese übermitteln. Dann teilen ihnen die Unternehmen lediglich Kriterien mit, aufgrund derer Adressportfolios zusammengestellt werden. Der Versand der Werbematerials erfolgt oft durch beauftragte Unternehmen, die sog. Lettershops.

Wie diese Vorgänge datenschutzrechtlich einzuordnen sind, ist bisher weder in Deutschland noch auf europäischer Ebene geklärt. Die DS-GVO enthält keine ausdrückliche Regelung zur Zulässigkeit postalischer Direktwerbung und des damit im Zusammenhang stehenden Adresshandels. Lediglich im Erwägungsgrund 47 Satz 7, einer Auslegungsregel zur DS-GVO, heißt es, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine Datenverarbeitung angesehen werden kann, die einem „berechtigten Interesse" dient. Unklar aber bleibt, was genau als Direktwerbung anzusehen ist und wie die Interessen der Werbeadressart*innen dabei zu berücksichtigen sind.

Dies alles führt unweigerlich zu Rechtsunsicherheit und Meinungsverschiedenheiten. Die Österreichische Datenschutzbehörde und der Dialog Marketing Verband Österreich gehen davon aus, dass Direktmarketing als ein berechtigtes Interesse gemäß Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO anzusehen ist. Dabei stützen sie sich auf eine seit Jahren in der österreichischen Gewerbeordnung verankerte Regelung, die das Direktmarketing unter Verwendung von personenbezogenen Daten aus öffentlichen Verzeichnissen durch Adressverlage und Direktmarketingunternehmen erlaubt. Demgegenüber ist in Deutschland nach Inkrafttreten der DS-GVO eine den Adresshandel begünstigende Vorschrift im BDSG nicht wieder übernommen worden. Die deutschen Datenschutzaufsichtsbehörden gehen deshalb mehrheitlich davon aus, dass jedenfalls der Handel mit Adressen und die postalische Direktwerbung dann einer Einwilligung der betroffenen Personen bedürfen, wenn sie nicht vom werbenden Unternehmen mit selbst erhobenen Daten eigener Kund*innen durchgeführt, sondern als eigenständige Dienstleistung angeboten werden.

Die LDI NRW lehnt den Standpunkt von Österreich jedenfalls nicht vollständig ab und hält es hingegen unter bestimmten Voraussetzungen für zulässig, die Verarbeitung personenbezogener Daten im Rahmen von Adresshandel und postalischer Direktwerbung auch ohne Einwilligung zu betreiben – gestützt auf die Rechtsgrundlage des Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO. Ein berechtigtes wirtschaftliches Interesse der Adresshändler, Direktmarketing zu ermöglichen oder werbetreibende Unternehmen bei ihrem Dirketmarketing zu unterstützen, damit diese ihre Waren und Dienstleistungen den Verbraucher*innen möglichst zielgerichtet anbieten können, ist vorhanden. Bei entsprechenden Rahmenbedingungen kann dieses berechtigte Interesse die möglicherweise entgegenstehenden Interessen der Adressaten überwiegen.

Noch ist dieser Diskussionsprozess zwischen den beteiligten Behörden nicht abgeschlossen. Zwar sind mittlerweile Änderungen an dem österreichischen Entwurf erfolgt. Die Kernfrage des Einwilligungserfordernisses ist aber weiterhin umstritten und nicht geklärt. Nach mehrheitlicher Auffassung der deutschen Datenschutzaufsichtsbehörden wäre der österreichische Entwurf deswegen als verbindliche transnationale Verhaltensregel nicht genehmigungsfähig.

Abzuwarten ist, ob die Österreichische Datenschutzbehörde ihr Vorhaben in die zuständigen Gremien des EDSA einbringen wird, um den Standpunkt weiterer europäischer Aufsichtsbehörden einzuholen. Die LDI NRW würde diese Klärung auf europäischer Ebene begrüßen und würde sich gemeinsam mit den anderen deutschen Behörden aktiv an diesem Diskussions- und Meinungsbildungsprozess beteiligen.

Fazit

Die Zulässigkeit der Verarbeitung personenbezogener Daten zum Zwecke der postalischen Direktwerbung ist umstritten, wenn Adresshändler und Dienstleitungsunternehmen ins Spiel kommen. Die österreichische Initiative trägt dazu bei, wichtige Fragen zu bearbeiten. Die LDI NRW begrüßt die eingeleitete Klärung auf europäischer Ebene.

11.3. Wenn Banken die Zahlungsverkehrsdaten zu Werbezwecken nutzen



Kreditinstitute dürfen Kund*innendaten einsetzen, um auf sich aufmerksam zu machen. Eine zielgerichtete Werbung, weg vom Gießkannenprinzip, kann dabei auch dem Interesse mancher Kund*innen dienen. Die Kernfrage ist aber: In welchem Umfang sind automatisierte Analysen ohne Einwilligung der Betroffenen erlaubt?

Smart Data, also „schlaue Daten", sind Datensätze, die für einen effizienten Einsatz aufbereitet wurden. Sie dienen Unternehmen etwa dazu, aus einem Kundenbestand gezielt Personen für bestimmte Werbemaßnahmen herauszufiltern. Auch in der Kreditwirtschaft kommen derartige Verfahren zum Einsatz. Die deutschen Datenschutzaufsichtsbehörden beschäftigen sich schon länger mit diesem Thema. 2024 nahm sich die LDI NRW nun die Volks- und Raiffeisenbanken in NRW vor. Das Ergebnis zeigt: Die geprüften Institute halten sich aktuell an die Regeln.

Die LDI NRW leitet den entsprechenden Arbeitskreis Kreditwirtschaft der DSK. Schon früh spielten Smart-Data-Verfahren dort eine Rolle. Während die Sparkassen-Finanzgruppe bereits im Jahre 2019 für die automatisierte Analyse von Bankdaten für Werbezwecke eine Einwilligungserklärung mit dem DSK-Arbeitskreis Kreditwirtschaft abstimmen konnte, ist dies mit der genossenschaftlichen Finanzgruppe aber erst Anfang 2023 gelungen. 2024 folgte dann die Prüfung der Volks- und Raiffeisenbanken.

Bei den Smart-Data-Verfahren in der genossenschaftlichen Finanzgruppe handelt es sich um komplexe Algorithmen zur Selektion von Kund*innendaten, die unter anderem Zahlungsverkehrsdaten und Wohnumfeld-Informationen einbeziehen. Anhand der gewonnenen Informationen wird entschieden, welche Art von Werbung Kund*innen erhalten sollen. Bis in das Jahr 2022 hatte der zuständige Bundesverband der Deutschen

Volks- und Raiffeisenbanken die Auffassung vertreten, dass überwiegend keine Einwilligungen der Kund*innen eingeholt werden müssten, sondern mittels einer sog. Hinweislösung gearbeitet werden könne. Dabei werden die betroffenen Personen lediglich per Informationsblatt auf die Verarbeitung ihrer personenbezogenen Daten hingewiesen.

Die Datenschutzaufsichtsbehörden sind hingegen der Auffassung, dass Zahlungsverkehrsdaten sowie die von Bankkund*innen genutzten Online-Banking-Geräte nur auf Einwilligungsbasis für werbliche Zwecke analysiert werden dürfen. Unter Zahlungsverkehrsdaten fallen vor allem der Verwendungszweck einer Zahlung, die Angaben zur zahlenden Person sowie zu den Zahlungsempfänger*innen. Bereits im 27. Datenschutzbericht 2022 hat sich die LDI NRW mit der datenschutzrechtlichen Beurteilung, ob und in welchem Umfang Kreditinstitute Daten ihrer Kund*innen für Werbezwecke nutzen dürfen, auseinandergesetzt. Die LDI NRW hat sich dahingehend positioniert, dass bei der werblichen Nutzung der besonders sensiblen Zahlungsverkehrsdaten grundsätzlich eine entsprechende Einwilligung der Kund*innen nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a der DS-GVO einzuholen ist.

Im Hinblick auf das von der niedersächsischen Datenschutzaufsichtsbehörde verhängte Bußgeld im Jahr 2022 gegen ein Kreditinstitut aus der genossenschaftlichen Finanzgruppe und der daraufhin erfolgten Warnung gegen weitere Kreditinstitute in Niedersachsen hatte sich die LDI NRW entschieden, auch die Kreditinstitute mit Sitz in NRW hinreichend zu sensibilisieren. Im Sommer 2024 dann wurden die Volks- und Raiffeisenbanken in NRW im Rahmen einer Prüfaktion detailliert befragt, ob sie sich an die Vorgaben des Austauschs zwischen der LDI NRW und den Kreditinstituten gehalten haben.

Die ausgewählten Kreditinstitute waren kooperativ und haben bereitwillig Auskunft erteilt. Dabei stellte sich erfreulicherweise heraus, dass alle befragten Kreditinstitute bereits spätestens seit Herbst 2022 für ihre Smart-Data-Analysen die Einwilligung ihrer Kund*innen einholen. Datenverarbeitungsvorgänge mittels Hinweislösung wurden vorsorglich freiwillig eingestellt. Außerdem kommen seither die mit den Datenschutzaufsichtsbehörden abgestimmten Muster der Einwilligungserklärung zum Einsatz.

Fazit

Die DS-GVO setzt Unternehmen, die besonders sensible Daten verarbeiten, sehr enge Grenzen bei der werblichen Nutzung von Kund*innendaten. Rechtsicherheit erlangen Kreditinstitute, wenn sie der Empfehlung der LDI NRW folgen und eine datenschutzkonforme Einwilligung der Kund*innen einholen. Wichtige Zweifelsfragen sollten mit der LDI NRW rechtzeitig im Dialog gelöst werden, um empfindliche Bußgelder zu vermeiden.

11.4. Dreiste Werbung – LDI NRW leitet Bußgeldverfahren gegen Telekommunikationsunternehmen aus NRW ein

Das Geschäftsgebaren eines Telekommunikationsunternehmens aus NRW hat zu Konsequenzen geführt. Da die Datenschutzrechte von Betroffenen massiv verletzt wurden, könnte es nun teuer für den Anbieter werden.

Die Beschwerden rissen nicht ab. Seit 2022 wandten sich immer wieder Verbraucher*innen aus demselben Grund an die LDI NRW: Sie erhielten nicht nur personalisierte Werbeschreiben eines Telekommunikationsunternehmens aus NRW, in dem ein Vertrag für einen Internet- und Telefonanschluss angepriesen wurde. Die Betroffenen gaben auch durchweg an, niemals zuvor Kontakt zu diesem Unternehmen gehabt zu haben.

Die Werbeschreiben waren sehr detailliert. Sie enthielten zum einen die Adresse und die Festnetztelefonnummer der Betroffenen. Zum anderen wurde ein mit Namen, Adresse und Anschluss vorausgefüllter Auftrag zum Abschluss des angebotenen Tarifs mit dem Unternehmen und zur Kündigung des Vertrags bei dem aktuellen Telekommunikationsanbieter mitgeliefert. Die Angeschriebenen sollten nur noch die IBAN ergänzen und den Auftrag unterschreiben. Hinzu kam ein weiterer Trick: durch die Aufmachung der Schreiben und die Namensähnlichkeit zu einem anderen Telekommunikationsunternehmen war vielen Verbraucher*innen nicht bewusst, dass es sich nicht um ein Angebot für einen (anderen) Tarif bei ihrem bisherigen Anbieter handelte – sondern um das Angebot zum Anbieterwechsel. Die Folge: Oft unterschrieben Betroffene die Vertragsunterlagen. Erst als sie später den Anbieterwechsel bemerkten, kündigten oder widerriefen sie die Verträge – und wurden dann von dem Unternehmen mit der Forderung einer Schadensersatzpauschale überzogen.

Wegen dieses Geschäftsgebarens haben einige Verbraucherzentralen bereits Gerichtsverfahren gegen das Unternehmen wegen vertrags- oder wettbewerbsrechtlicher Verstöße angestrengt und erfolgreich Urteile erstritten. Nach Überprüfung des Falles im vergangenen Jahr zog auch die LDI NRW Konsequenzen zu Lasten des Telekommunikationsanbieters und leitete ein Geldbuße-Verfahren ein. Die LDI NRW beabsichtigt außerdem Anweisungen zu treffen, die die Datenverarbeitung des Unternehmens mit dem Datenschutzrecht in Einklang bringen sollen.

Dabei ist zu berücksichtigen, dass die LDI NRW für diese Fälle nicht allumfassend zuständig ist. Für die Branche der Telekommunikationsanbieter gibt es eine Spezialzuständigkeit, grundsätzlich ist hier die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die richtige Aufsichtsbehörde, soweit es um die Erbringung der

Telekommunikationsdienstleistung geht. Beschwerden, in denen ein Vertragsschluss mit dem Unternehmen erfolgte oder behauptet wird, liegen deshalb in der Zuständigkeit der BfDI und werden an diese abgegeben.

Hinsichtlich der datenschutzrechtlichen Aspekte beschwerten sich die Verbraucher*innen bei der LDI NRW vor allem über das ignorante Verhalten des Unternehmens. Das antwortete den Betroffenen weder auf geltend gemachte Auskunftsansprüche über die Verarbeitung ihrer Daten noch auf den Wunsch nach Löschung oder auf ihre Widersprüche gegen die Verarbeitung der Daten. Und das, obwohl die Schreiben oder E-Mails entgegen der Aussagen des Unternehmens vielfach nachweisbar dort zugegangen waren. Zudem enthielten die versandten Werbeschreiben nicht die vorgeschriebenen Informationen bei einer Datenverarbeitung, etwa Angaben zum Verantwortlichen für die Datenerhebung und den Datenschutzbeauftragten. Auch blieb das Unternehmen regelmäßig intransparent beim Nachweis der Herkunft der Daten.

Die Beschwerdeverfahren verliefen zusätzlich sehr schleppend. Trotz klarer gesetzlicher Vorschriften zur Mitwirkung und vieler Erinnerungen verhielt sich das Unternehmen gegenüber der LDI NRW nur eingeschränkt kooperativ. Es berief sich in der Sache auf ein angebliches berechtigtes Interesse zur Datenverarbeitung, konnte der LDI NRW aber in keinem Fall nachweisen, dass es die notwendige Abwägung mit den Interessen der Betroffenen durchgeführt hätte.

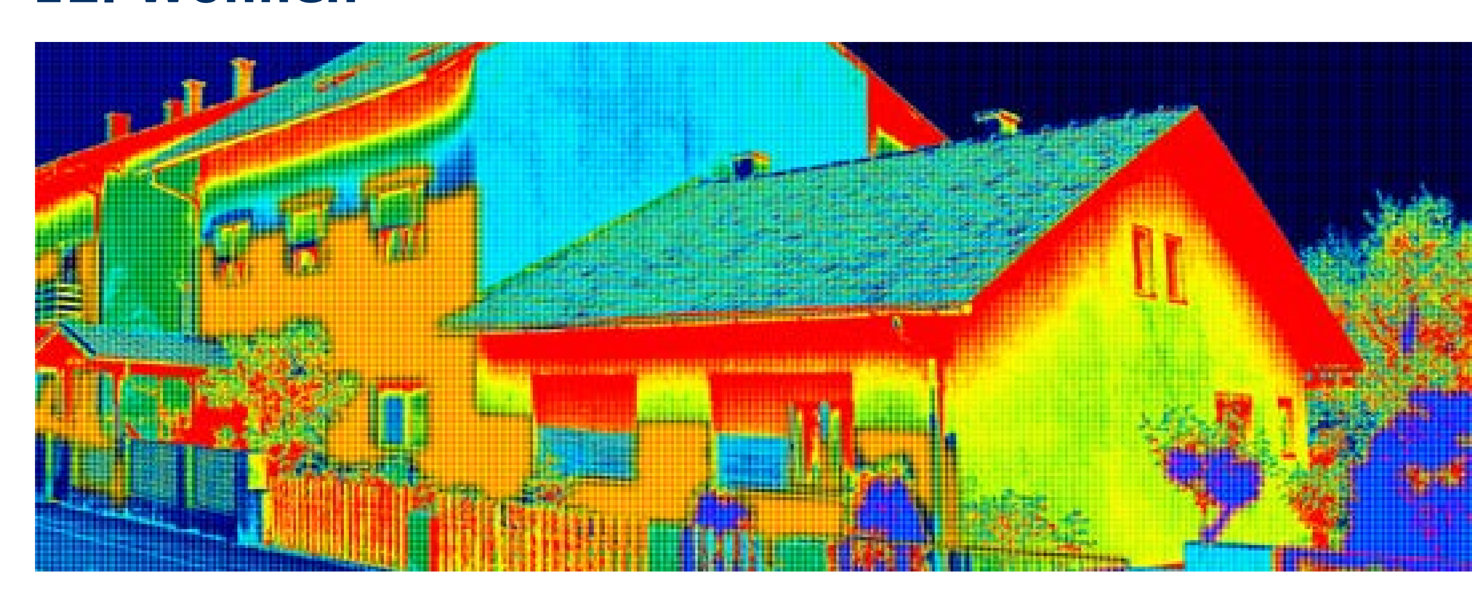
Dies wäre überdies auch nicht erfolgversprechend gewesen. Zwar kann die Nutzung von Adressen für Werbezwecke grundsätzlich als ein berechtigtes Interesse eines Werbetreibenden angesehen werden. Nicht erforderlich dafür ist jedoch eine auf dem Werbeschreiben aufgedruckte Telefonnummer. Im konkreten Fall trug deren Aufdruck sogar zur Irreführung der Betroffenen bei, da sie wegen der Namensähnlichkeit des werbenden Unternehmens mit ihrem aktuellen Anbieter davon ausgingen, dass dieser sie angeschrieben hatte. Das Interesse Betroffener daran, dass ihre Daten nicht für wettbewerbswidrige Werbung genutzt werden, überwiegt aber regelmäßig die Interessen des dafür verantwortlichen Unternehmens.

Die Wettbewerbswidrigkeit dieses Verhaltens wird mittlerweile auch durch die von einigen Verbraucherzentralen erstrittenen Urteile gegen das Unternehmen bestätigt. Die LDI NRW hat zusätzlich wegen der Verstöße gegen die Betroffenenrechte ein Geldbuße-Verfahren gegen das Unternehmen eingeleitet. Außerdem sollen weitere Maßnahmen getroffen werden, damit das Unternehmen zukünftig wesentliche Grundsätze für die Verarbeitung personenbezogener Daten einhält und seiner Pflicht zur Rechenschaft nachkommt. Dies betrifft insbesondere die Rechtmäßigkeit und die Transparenz der Datenverarbeitung.

Fazit

Will ein Unternehmen personalisierte Schreiben für Werbezwecke einsetzen, sollte es penibel auf die Datenschutzrechte der Angeschriebenen achten. Ein Verstoß gegen deren Rechte sowie eine hartnäckige Weigerung zur Änderung dieses Verhalten kann empfindliche finanzielle Konsequenzen haben.

12. Wohnen



12.1. Wärmebilder von Häusern können beim Energieeinsparen helfen – wenn die Rechte der Nachbar*innen beachtet werden

Wärmebildaufnahmen von Fassaden zeigen Haus-Eigentümer*innen, wo noch Energie eingespart werden kann. Und sie nutzen Unternehmen, die entsprechende Wärmelandkarten erstellen, um Haus-Eigentümer*innen von ihren Angeboten für energetische Sanierungen zu überzeugen. Doch ganz so einfach funktioniert das Geschäft nicht.

Der Hinweis kam 2024 durch eine Presseanfrage. Ein Journalist wollte etwas zu einem Versorgungsunternehmen wissen. Das hatte vor, in NRW Straßen abzufahren, um von Wohngebäuden mittels Kamera Wärmebilder anzufertigen und so Energiesparpotentiale aufzuzeigen. Über diese energetischen Fotoaufnahmen sollten dann sanierungsinteressierten Gebäude-Eigentümer*innen Dienstleistungen angeboten werden.

Die nachfolgenden Ermittlungen der LDI NRW ergaben folgendes Bild: Die Aufnahmen werden durch ein mit Thermalkameras ausgestattetes Fahrzeug erstellt, das alle sichtbaren Gebäudeteile an der Vorderfront erfasst. Die Aufnahmen sind auf die straßenseitige Ansicht begrenzt, für die rückwärtigen Ansichten kommen keine Drohnen zum Einsatz. Die Thermalbilder werden dann mithilfe frei verfügbarer Daten zum Gebäudebestand (etwa über die Zensusdaten) ausgewertet. So entsteht eine Wärmelandkarte, auf der die energetischen Zustände der Wohngebäude zu sehen sind.

Um Rückschlüsse auf Eigentümer*innen und Bewohner*innen der Wohngebäude völlig auszuschließen, werden immer mindestens drei Gebäude zu einer Darstellung zusammengeführt. Die Eigentümer*innen-Stellung wird erst dann konkret, wenn es um die Abfrage einer Dienstleistung geht. Bei der Angebotserstellung werden dann die Nachbargebäude geschwärzt, denn der Gebäudezustand nebenan geht die Person nichts an, die ihr eigenes Haus gern sanieren möchte.

Damit möglichst alle betroffenen Personen von dem Vorhaben erfahren, verbreitete das Versorgungsunternehmen im Vorfeld der Wärmebildfahrten über verschiedene Wege Informationen dazu. Danach soll ein Widerspruch gegen die Datenverarbeitung für ein bestimmtes Gebäude jederzeit und voraussetzungslos möglich sein. Bei Widersprüchen, die nach Erstellung der Wärmebildaufnahmen eingelegt werden, soll eine bis dahin erfolgte Verarbeitung der Bilder rückgängig gemacht werden.

Aber ist das genug, um das Vorhaben als datenschutzkonform zu bewerten? Die LDI NRW sieht es jedenfalls als erforderlich an, dass potentiell datenschutzrelevante Aspekte des Projekts ermittelt und entsprechende Schutzmaßnahmen ergriffen werden.

Grundsätzlich sind sowohl das Einsparen von Energie als auch deren optimierte Nutzung bedeutende gesellschaftliche und umweltpolitische Themen. Projekte wie das des betroffenen Versorgungsunternehmens können dabei eine wichtige Hilfe sein. Datenschutzrechtlich sollte bei der Umsetzung jedoch bedacht werden, dass durch die Kamerafahrten, die spätere Auswertung der Bilder, die Zusammenfassung mit frei verfügbaren weiteren Daten sowie die Darstellung auf einer Wärmelandkarte möglicherweise personenbezogene Daten erfasst und verarbeitet werden.

Für eine datenschutzkonforme Umsetzung dieses Vorhabens ist es daher entscheidend, dass verschiedene Aspekte Berücksichtigung finden:

- Unternehmen können durchaus Gebäudefassaden mittels Thermalkamera erfassen und Bildaufnahmen von öffentlichem Straßenraum publizieren – ohne dass dafür die Einwilligung betroffener Personen erforderlich wäre. Als Rechtsgrundlage kommt Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO in Betracht. Hiernach darf ein Unternehmen personenbezogene Daten verarbeiten, sofern dies zur Wahrnehmung berechtigter Interessen erforderlich ist und nicht die Interessen der betroffenen Person überwiegen. In einem solchen Fall ist aber eine umfassende Interessenabwägung unumgänglich. Diese ist zu dokumentieren. Darüber hinaus sind Schutzmaßnahmen zu ergreifen, um die Sicherheit von personenbezogenen Daten zu gewährleisten. Dagegen kommt der von dem Energieversorger angeführte § 59 des Urhebergesetzes nicht als Rechtsgrundlage in Betracht. Er erlaubt zwar Fotografien von der äußeren Ansicht eines Gebäudes, aber nicht die Erfassung

und Auswertung des energetischen Gebäudezustandes. Denn diese Art der Erfassung geht über die Abbildung der reinen Fassadenansicht hinaus.

- Im Vorfeld der Kamerafahrten muss umfassend informiert werden, über das geplante Projekt an sich, die Kamerafahrten (möglichst mit einem genauen Zeitfenster, in dem diese stattfinden sollen), über die Erfassung und weitere Verarbeitung der Bilder, aber auch über Widerspruchsmöglichkeiten und Ansprechparner*innen. Diese Informationen sollten sowohl breit gestreut werden mittels Zeitung, Sozialer Medien, Funk und Fernsehen; als auch direkt vor Ort verbreitet werden, etwa über Postwurfsendungen, Handzettel und Aushänge bei den Bewohner*innen. Eine hohe Transparenz der geplanten Datenverarbeitung steht nicht nur im Einklang mit dem Daten schutz. Sie kann auch zur Akzeptanz des geplanten Projekts beitragen und etwaige Beschwerden im weiteren Verfahren reduzieren.

- Auch wenn nur sog. Thermalkameras eingesetzt werden, die keine Gesichter, Hausnummern oder KFZ-Kennzeichen erfassen, sollten nur die reinen Straßenansichten der Gebäude aufgenommen werden und allein diese Werte in die Wärmelandkarte einfließen. Drohnenbilder bzw. Filme von Privatbereichen der Gebäude sind tabu. Durch diese Einschränkungen sind die Gefahren für die Erfassung personenbezogener Daten im Rahmen der Kamerafahrten deutlich reduziert. Allerdings ist auch in diesem Projektschritt darauf zu achten, dass möglichst wenige personenbezogene Daten durch die Kameras erhoben werden. Denn bei der Vorbeifahrt des Kamerafahrzeugs könnten etwa auch unbeteiligte Dritte mit ihren Thermalmerkmalen erfasst werden. Sollte es zu Aufnahmen von Personen oder Fahrzeugen kommen, so sind diese unverzüglich zu löschen oder nachhaltig zu schwärzen. Für die energetische Bewertung der Gebäudefronten sind derartige Aufnahmen nicht weiter von Belang und deren Vorhalten oder gar die weitere Verarbeitung grundsätzlich datenschutzwidrig.

- Notwendig ist auch, die Anzahl der Gebäude sorgfältig auszuwählen, die für die öffentlich einsehbare Wärmelandkarte zusammengefasst werden und deren energetischer Stand kumuliert angezeigt wird. Denn je nach Wohngebiet lassen sich ansonsten trotzdem Rückschlüsse auf den energetischen Zustand einzelner Gebäude oder Wohnungen ziehen. So kann es sein, dass etwa in einem Gebiet mit Einfamilienhäusern durchaus mehr Gebäude zu einer Einheit auf der Wärmelandkarte zusammengefasst werden müssen, als dies etwa bei einer zusammenhängenden Bebauung der Fall wäre. Auf einer eng bebauten Strecke, sind die einzelnen Streckenabschnitte weniger leicht rekonstruierbar, als dort wo bei großen Gebäudeabständen leicht erkennbar ist, welche drei Gebäude zusammengefasst wurden.

- Ein weiterer wichtiger Punkt zum Schutz der Daten von Hauseigentümer*innen ist das umfassende, voraussetzungslose und zu jeder Zeit mögliche Widerspruchsrecht gegen die Datenverarbeitung. Sollte der Widerspruch erst nach Erstellung der Wärmebildaufnahmen erfolgen, so ist die bis dahin erfolgte Verarbeitung rückgängig zu machen und sind die entsprechenden Daten unwiderruflich zu löschen.

- Der Betreiber einer Wärmelandkarte sollte wissen, dass er verpflichtet ist, die Aktualität der entsprechenden Daten sicherzustellen. Denn folgen auf die energetischen Erhebungen später entsprechende Sanierungsarbeiten, ändern sich womöglich die Grunddaten zu einzelnen Immobilien erheblich. Dies kann wiederum Einfluss auf die Daten in der Wärmelandkarte haben. Neben dem allgemeinen Interesse an der Richtigkeit der öffentlichen Wärmelandkarte dürften betroffene Eigentümer*innen ein nicht unerhebliches Eigeninteresse an der korrekten Darstellung der kumulierten Einheit haben.

Fazit

Datenschutz und Energieberatung können harmonisch gelingen, wenn von Anfang an gut geplant wird. Das von uns geprüfte Unternehmen hatte hierzu bereits wichtige eigene Schritte unternommen. Diese Schritte und die hier von uns gegebenen weiteren Hinweise können auch zum Erfolg vergleichbarer Projekte beitragen.

12.2. Smart Metering: Neue Orientierungshilfe hilft im Umgang mit funkbasierten Strom-, Heizungs- und Wasserzählern



Wenn die Energie-Zähler zuhause Daten sammeln können, wächst die Verunsicherung bei Verbraucher*innen, Hausverwaltungen und Hersteller*innen. Zur besseren Information haben die deutschen Datenschutzaufsichtsbehörden deshalb eine Orientierungshilfe zum Thema Smart Metering veröffentlicht. Das Papier erklärt anschaulich, wie die rechtmäßige Datenverarbeitung beim Einsatz dieser Zähler funktioniert.

Häuser oder Wohnungen in Deutschland werden zunehmend schlauer, eben „smarter". Ob Strom-, Heizungs- oder Wasserverbrauch – die digitale Erhebung und Verarbeitung von Verbrauchsdaten wird derzeit nach und nach flächendeckend funkgesteuert und fernauslesbar umgestaltet. Bürger*innen soll dadurch das Einsparen von Energie erleichtert werden. Sie können mit der neuen Technik ihre Energieverbräuche genauer im Blick behalten und erhalten nicht erst durch eine jährliche Abrechnung ihres Versorgers davon Kenntnis.

Das ist die Intention des europäischen Gesetzgebers, die mit der Energieeffizienzrichtlinie für die Strom- sowie Heizungs- und Warmwasserzähler festgeschrieben wurde. Die Richtlinie wurde mittlerweile in deutsches Recht umgesetzt. Deutsche Umsetzungsregelungen finden sich im Messstellenbetriebsgesetz (MsbG), in der Verordnung über die Heizkostenabrechnung (HeizkostenV) und in der Fernwärme- oder Fernkälte-Verbrauchserfassungs- und -Abrechnungsverordnung (FFVAV).

Doch mit der neuen funkbasierten Datenverarbeitung geht zugleich Verunsicherung einher. Einerseits wollen Bürger*innen wissen, wie ihre Verbrauchsdaten geschützt werden und wer diese Daten verwendet. Manche sorgen sich, dass ihre Daten von Fremden ausgelesen werden

könnten, die daraus Rückschlüsse darauf ziehen, ob ein Haus etwa ferienbedingt keinen oder wenig Verbrauch hat – und deshalb ein geeignetes Diebstahlsziel ist. Andere wollen sichergestellt wissen, dass ihre Verbrauchsprofile beispielsweise nicht für Werbezwecke genutzt werden.

Andererseits bestehen auch Unklarheiten bei Eigentümer*innen, Haus- und Wohnungsverwaltungen sowie bei den Geräteherstellern, Energieversorgern und Ableseunternehmen selbst. Diese sind nämlich in der Pflicht, den Verbraucher*innen die notwendigen Antworten auf Fragestellungen zur Verfügung zu stellen, die mit dem Einsatz von Smart Metern einhergehen. Kompliziert macht die Situation zusätzlich, dass der datenschutzrechtliche Regelungsrahmen je nach Energieart unterschiedlich oder zum Teil gar nicht vorhanden ist.

Die DSK hat deshalb die Orientierungshilfe „Datenverarbeitung im Zusammenhang mit funkbasierten Zählern" vom 16.08.2024 herausgegeben, abrufbar unter www.datenschutzkonferenz-online.de/orientierungshilfen. Vorbereitet wurde diese Orientierungshilfe unter Federführung der LDI NRW. Sie beantwortet ausführlich Fragen im Zusammenhang mit der Rechtmäßigkeit der funkgesteuerten Erhebung und Übermittlung von Verbrauchsdaten. Ziel ist es, den technischen Fortschritt zu unterstützen – ohne dass der Datenschutz zu kurz kommt. In dem nach Fragestellungen aufgebauten Papier werden übersichtlich die Rechtsgrundlagen für die Installation funkbasierter Zähler, die weitere Verarbeitung der Verbrauchsdaten, das Zusammenspiel beteiligter Akteure sowie das Thema Datensicherheit dargestellt und damit viele Fragen beantwortet.

Die LDI NRW wird diesem Komplex auch weiterhin viel Aufmerksamkeit widmen. Derzeit wird ein Code of Conduct (CoC), ein Verhaltenskodex, von einem Verband der Messgerätehersteller auf seine Genehmigungsfähigkeit hin untersucht. Die Messgerätehersteller handeln sehr oft auch als Auftragsverarbeiter für Wohnungsvermieter*innen. Der CoC der Messgerätehersteller soll branchenspezifische Regeln für den datenschutzkonformen Umgang mit Verbrauchsdaten durch die Hersteller von Messgeräten bei ihrer Auftragsverarbeitung beschreiben. Auch dies kann zu Transparenz und zum datenschutzgerechten Umgang mit Verbrauchsdaten beitragen.

Fazit

Die neue Orientierungshilfe der DSK ist eine wertvolle Unterstützung für alle Beteiligten im datenschutzkonformen Umgang mit Smart-Meter-Gateways. Insbesondere Bürger*innen ist es nun auch leichter möglich, sich umfassend zu funkbasierten Zählern zu informieren.

12.3. Stadtwerke sollten WhatsApp nicht beim Zählerablesen einsetzen

Stromversorger ermöglichen es ihren Kund*innen teilweise, Zählerstände in ihren Haushalten auch über den Messenger-Dienst WhatsApp mitzuteilen. Aber ist das überhaupt sicher und datenschutzrechtlich erlaubt? Die LDI NRW rät aus verschiedenen Gründen davon ab.

Es gehört zur jährlich wiederkehrenden Aufgabe in Millionen deutscher Haushalte: das Ablesen von Stromzählern und das Mitteilen der Zählerstände an das Versorgungsunternehmen. Wurden früher vorgefertigte Postkarten dafür benutzt, funktioniert dies heute meist per QR-Code, der auf die Internetseite des Unternehmens führt. Doch die Entwicklung der Kommunikation geht noch weiter. Stromversorger setzen teilweise jetzt auch auf den Messenger-Dienst WhatsApp, mit dessen Hilfe der Zählerstand übermittelt werden kann.

Nicht allen Kund*innen ist dies allerdings geheuer. So erreichte die LDI NRW im Jahr 2024 eine Beschwerde zu dieser vermeintlich modernen Ablese- bzw. Meldemethode. Die Beschwerdeführerin war Anfang Juli des vergangenen Jahres aufgefordert worden, ihren Zählerstand mitzuteilen – wobei ihr neben dem bisher üblichen Vorgehen auch die Möglichkeit angeboten wurde, den Zählerstand per Messenger-Dienst WhatsApp an eine auf dem Mitteilungszettel handschriftlich notierte Mobilfunknummer zu übermitteln. Dies war auf dem Zettel im Fettdruck hervorgehoben.

Nicht ersichtlich war jedoch, wem die Telefonnummer konkret zuzuordnen war. Die Beschwerdeführerin rügte daher, dass sie nicht nachvollziehen könne, ob die Telefonnummer wirklich zu den Stadtwerken gehöre oder auf eine andere Person zugelassen sei. Weitergehende Hinweise zur Datenverarbeitung fanden sich auf dem Mitteilungszettel nicht.

Die LDI NRW hat den Fall untersucht und den Stadtwerken von der WhatsApp-Methode abgeraten. Die Stadtwerke haben daraufhin auf den weiteren Einsatz verzichtet, obwohl sie selbst weiterhin keine Bedenken gegen die Nutzung eines Messenger-Dienstes hatten. Die LDI NRW hat daraufhin gegenüber den Stadtwerken noch einmal die Rechtslage klargestellt. Auch andere Dienstleister, die Ähnliches planen, sollten diese Rechtslage berücksichtigen – insbesondere auch mit Blick darauf, dass selbst eine freiwillige Nutzung durch die Verbraucher*innen an der Einschätzung nichts ändert.

Problematisch ist zunächst, dass für die Nutzer*innen-Identifikation Telefonnummern zum Einsatz kommen und dabei das vollständige Adressbuch an den Anbieter des Messenger-Dienstes übermittelt wird, im

Fall von WhatsApp an den US-Konzern Meta. Dadurch werden die im Adressbuch des Nutzers enthaltenen anderen Nutzer*innen des Dienstes identifizierbar. Dieses „Match-Making" erlaubt WhatsApp/Meta, all diese Daten für eigene Zwecke zu benutzen. Geht die Nutzung aber über rein private oder familiäre Zwecke hinaus, sind mangels einer gesetzlichen Erlaubnis für die Weitergabe der Daten grundsätzlich die Einwilligungen aller Personen einzuholen, deren Telefonnummern im Adressbuch gespeichert sind – was im konkreten Fall nicht geschehen ist und generell kaum machbar erscheint.

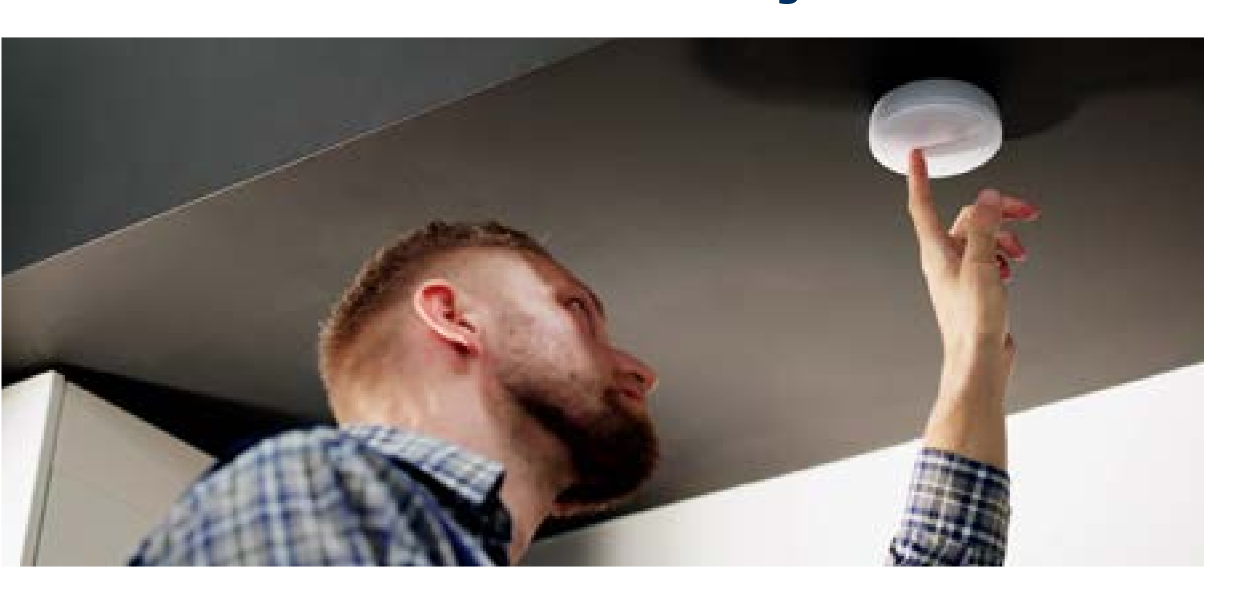
Hinzu kommt, dass die Stadtwerke für eine sichere Löschung von Daten sorgen müssten. Zwar ist positiv zu bewerten, dass Chat-Nachrichten bei WhatsApp grundsätzlich Ende-zu-Ende-verschlüsselt werden. Der Nachrichteninhalt wird dadurch über alle Übertragungsstationen zum Empfänger verschlüsselt versendet. Häufig machen Nutzer*innen jedoch von der von WhatsApp angebotenen Möglichkeit Gebrauch, Chatverläufe durch ein Backup zu sichern, um etwa die Daten später auf ein neues Endgerät übertragen zu können. In diesem Fall liegen die Chat-Inhalte auf dem Server von WhatsApp/Meta. Zwar bietet WhatsApp inzwischen eine Verschlüsselung der Inhalte für das Backup an. Nutzer*innen wie die Stadtwerke, die WhatsApp geschäftlich verwenden, sind jedoch verpflichtet sicherzustellen, dass die Inhaltsdaten gelöscht werden, sobald die Verarbeitung zur Erreichung des legitimen Zwecks nicht mehr erforderlich ist. Dazu zählt auch, durch Voreinstellungen sicherzustellen, dass die Chat-Inhalte auch bei WhatsApp/Meta nicht dauerhaft gespei-chert werden.

Schließlich ist zu berücksichtigen, dass WhatsApp nach eigenen Angaben personenbezogene Metadaten der Nutzer*innen („Wer kommuniziert wann mit wem") an WhatsApp/Meta USA übermittelt. Der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat deshalb bereits im Jahr 2020 per Rundschreiben die Nutzung von WhatsApp für alle oberen Bundesbehörden und Bundesministerien ausgeschlossen. 2023 hat außerdem die irische Datenschutzbehörde (Data Protection Commissioner, DPC) gegenüber Meta angemahnt, dass WhatsApp in unzulässiger Weise personenbezogene Daten seiner Nutzer*innen zu Zwecken der Serviceverbesserungen und der Sicherheit verarbeitet. Noch steht eine abschließende Bewertung aus, ob die von WhatsApp getroffenen Abhilfe-Maßnahmen hinreichend sind, um den Beschluss der DPC umzusetzen. Der EDSA hat die DPC aufgefordert, zusätzlich zu untersuchen, ob WhatsApp sensible personenbezogene Daten für Zwecke der verhaltensbezogenen Werbung, für Marketingzwecke sowie für die Bereitstellung von Statistiken an Dritte und den Austausch von Daten mit verbundenen Unternehmen verarbeitet – und ob dies im Einklang mit der DS-GVO geschieht. Auch hier gibt es derzeit noch kein Ergebnis

Fazit

Wegen des regelmäßig stattfindenden Adressbuchabgleichs und der Intransparenz über Datenverarbeitungen durch Meta/WhatsApp zu eigenen Zwecken ist es Verantwortlichen aktuell kaum möglich, ihrer Rechenschaftspflicht nach der DS-GVO nachzukommen. Gerade Dienstleistungsunternehmen im Bereich der Daseinsvorsorge haben eine Vorbildfunktion, der sie nicht gerecht werden, wenn sie WhatsApp trotz der damit verbundenen Rechtsprobleme einsetzen.

12.4. Rauchmelder mit Klima-Monitoring müssen erst einmal ausgeschaltet sein



Neuste Technik hält auch in Wohnimmobilien Einzug. Beliebt bei Vermieter*innen sind vor allem Rauchwarnmelder, die zugleich das Klima prüfen können. Sie erheben Daten zur Raumtemperatur und Luftfeuchtigkeit und sind in der Lage, diese Daten an externe Dienstleister zu übermitteln. Doch müssen Mieter*innen das hinnehmen?

Herkömmliche Rauchwarnmelder sind der breiten Öffentlichkeit spätestens seit Änderung der Bauordnung NRW im Jahre 2013 und der damit verbundenen verpflichtenden Anbringung in Wohnräumen bekannt. Nun gibt es auch Warnmelder mit smarter Technologie. Die neueste Generation von Rauchwarnmeldern ermöglicht neben der Erkennung und Meldung von Brandereignissen mit Rauchentwicklung auch die Erhebung und Weitergabe von Daten zum Raum- und Klimamonitoring.

Diese Daten haben einen Personenbezug, weil sich daraus Erkenntnisse über das Verhalten der Bewohner*innen ableiten lassen. Neben dem Lüftungs- und Heizverhalten deutet plötzlich ansteigende Raumfeuchtigkeit etwa auf Kochen oder Duschen in der Wohnung hin. Auch die Anzahl der Personen, die sich in einer Wohnung aufhalten, beeinflusst die Daten.

Ein großes Wohnungsunternehmen mit Sitz in NRW hat die LDI NRW um Beratung zum datenschutzgerechten Einsatz solcher Warnmelder gebeten. Seitdem wenden sich auch vermehrt betroffene Mieter*innen mit Beschwerden und Beratungsbitten an die LDI NRW. Das Wohnungsunternehmen wurde darauf hingewiesen, dass die Melder nur mit ausgeschalteter Klima-Funktion installiert werden dürfen, damit die Mieter*innen die Wahl haben, ob sie die Zusatzfunktion der Geräte nutzen wollen oder nicht.

Das Unternehmen verspricht sich von der Installation und Nutzung gezielte Verhaltensempfehlungen für die Bewohner*innen, die über eine App transportiert werden – beispielsweise zum vermehrten Lüften der Wohnung. Mögliche Gefahren für die Gesundheit der Mieter*innen (etwa Schimmelbildung) oder Schäden an der Gebäudesubstanz könnten so im Vorfeld vermieden werden. Ebenso könne durch ein effizienteres individuelles Heizverhalten eine CO^2-Einsparung erreicht werden.

Die erhobenen Klimadaten (Temperatur und Luftfeuchtigkeit) können zweitweise am montierten Gerät gespeichert werden und optional – das heißt, wenn die Mieter*innen es wollen – in aufbereiteter Form für verschiedene Anwendungen, etwa in einer Mieter-App, zur Verfügung gestellt werden. Dabei ist die Übertragung personenbezogener Daten aus dem Gebäude heraus notwendig. Ähnliche Übertragungswege sind beispielsweise aus dem Bereich der Heizkostenablesung bekannt.

Diese technische Weiterentwicklung weckt bei Mieter*innen verständliche datenschutzrechtliche Vorbehalte. Welche Daten erhält die vermietende Partei, und wo werden meine Daten gespeichert? Was ist, wenn ich mit der Weitergabe der Daten nicht einverstanden bin?

Bei der Beratung hat die LDI NRW daher besonderes Augenmerk auf eine breite und transparente Information sowie einen ausgewogenen Schutz der betroffenen Personen gelegt, weil die Inbetriebnahme solcher Funktionen immer einen Eingriff in die eigene Wohnung darstellt. Nach der DS-GVO müssen Vermieter*innen ihre Mieter*innen vor der Installation über die Funktionen der neuen Geräte sowie über die mögliche Datenverarbeitung und insbesondere deren Zweck in transparenter Form informieren. So kann auch möglichen Ängsten der Mieter*innen begegnet werden.

Besonders hervorzuheben ist, dass die Verarbeitung der Raum- und Klimadaten einer rechtlichen Grundlage bedarf. Dies gilt bereits für die Erhebung und die gegebenenfalls nur kurze Speicherung von Daten im Gerät. Die Verarbeitung von Raum- und Klimadaten ist zulässig, wenn die Betroffenen ausdrücklich eingewilligt haben.

Haben Mieter*innen vor der Installation nicht in die Datenverarbeitung eingewilligt, dürfen Geräte mit solchen Zusatzfunktionen nur mit ausgeschalteter Klima-Funktion installiert werden. Bieten Rauchwarnmelder Funktionsmöglichkeiten, die über die gesetzlich vorgeschriebene reine Rauchwarnmeldung hinausgehen, müssen Mieter*innen selbst entscheiden können, ob sie diese zusätzlichen Funktionen nutzen und dann einschalten wollen. Für einen Mieter*innen-Wechsel heißt das, dass eingeschaltete Zusatzfunktionen vor dem Einzug wieder ausgeschaltet werden müssen, es sei denn, die neuen Bewohner*innen haben zuvor in die Datenverarbeitung eingewilligt. Diese Einwilligung ist allerdings nur wirksam, wenn sie informiert und freiwillig erteilt wurde. Das bedeutet vor allem auch, dass der Abschluss des Mietvertrages keinesfalls davon abhängig gemacht werden darf, dass eine Einwilligung in das Klimamonitoring erteilt wird. Die Einwilligung der Mieter*innen sollte daher regelmäßig erst mit Wohnungsübergabe angefragt werden, zu Nachweiszwecken am besten schriftlich.

Dabei ist zusätzlich zu beachten: Bereits mit dem Einschalten der Geräte werden personenbezogene Daten gesammelt und damit verarbeitet. Verfügen Geräte über zwei Aktivierungsmöglichkeiten, eine zum Einschalten der Zusatzfunktion, die andere zur Datenweiterleitung, müssen folglich beide Funktionen beim Einbau ausgeschaltet sein.

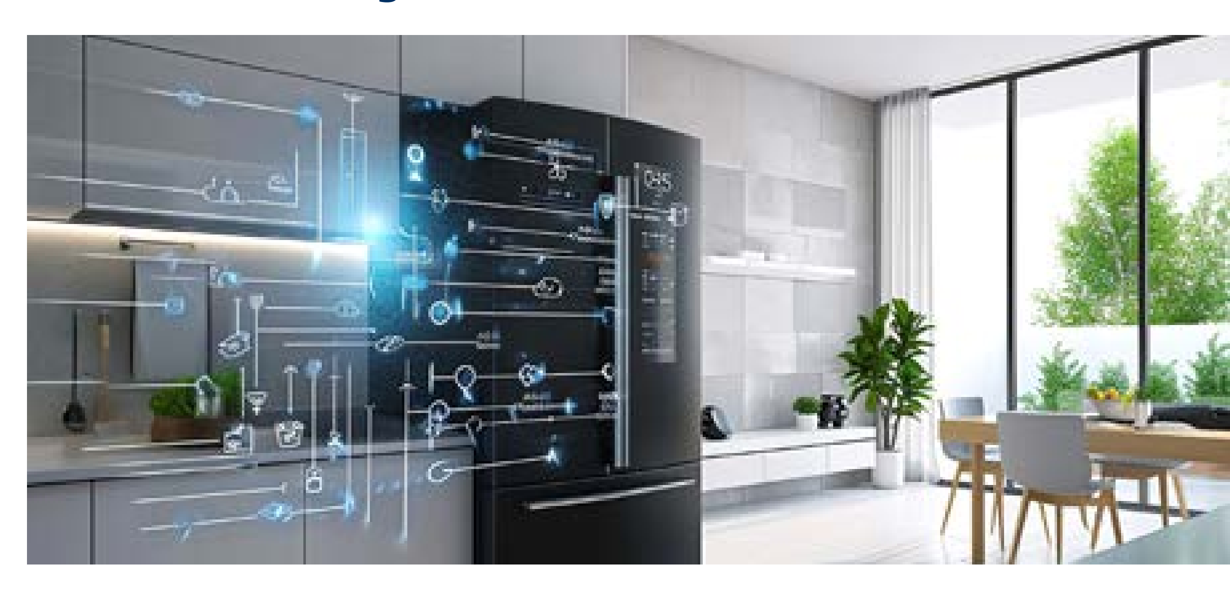
Vermieter*innen sollen die Daten zudem nur in anonymisierter Form und nicht wohnungsbezogen erhalten. Die Technik darf nicht zur Überwachung der Mieter*innen eingesetzt werden. Sie soll vielmehr die Mieter*innen im richtigen Lüftungs- und Heizverhalten unterstützen. Von regelmäßig gelüfteten Wohnungen profitieren dann alle Beteiligten.

In der Presse wurde darüber berichtet, dass Vermieter*innen den Einbau solcher smarten Warnmelder als Modernisierungsmaßnahme bei den Mietkosten berücksichtigen. Diese Frage war nicht Gegenstand unserer Prüfungen, da sie mietrechtlich und nicht datenschutzrechtlich zu beurteilen ist. Mit datenschutzrechtlichen Mitteln können nur unzulässige Datenverarbeitungen unterbunden werden. Gegen den Einbau einer ausgeschalteten technischen Anlage, mit der Daten nur potentiell erfasst werden können, stellt das Datenschutzrecht keine geeigneten Mittel zur Verfügung.

Fazit

Rauchwarnmelder mit Raum- und Klimamonitoring können Mieter*innen beim richtigen Lüftungs- und Heizverhalten unterstützen. Die dazu erforderliche Datenverarbeitung bedarf aber der Einwilligung der Mieter*innen, die informiert, zweckgebunden, freiwillig und widerrufbar sein muss. Beim Einbau der Geräte müssen alle Zusatzfunktionen ausgeschaltet sein. Die LDI NRW rät Vermieter*innen, sich an die genannten Vorgaben zu halten. Sofern sie Dienstleister*innen mit dem Einbau der Geräte beauftragen oder bereits beauftragt haben, müssen sie dafür Sorge tragen, dass diese die datenschutzrechtlichen Vorgaben beachten. Verstöße können mit empfindlichen Bußgeldern geahndet werden.

12.5. Smarte Geräte im Haushalt – Käufer*innen wie Hersteller*innen sollten Sorgfalt walten lassen



Lautsprecher, Fernseher, Fritteusen, Kameras oder Türklingeln, sie alle gibt es mittlerweile mit smarten Funktionen. Das lockt zum Kauf, denn die Geräte steigern den Komfort und lassen sich oft auch von unterwegs bedienen. Damit einher gehen allerdings viele Datenerhebungen und -verarbeitungen. Die LDI NRW rät zu Aufmerksamkeit – und ist mit den Hersteller*innen im Gespräch.

Smarte Produkte im Haushalt sind bei den Verbraucher*innen gefragt, schüren aber auch neue Ängste. Presseberichte wie der über smarte

Fritteusen, die angeblich ihre Nutzer*innen belauschen und sogar Audio-Daten nach China senden, führen immer wieder zu Fragen über mögliche Datenschutzverletzungen und ihre Konsequenzen.

Die LDI NRW hat sich deshalb 2024 intensiver mit dem Thema befasst und sich insbesondere angeschaut, was bei Herstellern zu beachten ist, die mit ihren smarten Geräten auch eine smarte Datenverarbeitung in ihrer Verantwortung anbieten. Sie rät Verbraucher*innen zu Aufmerksamkeit und mündigem Umgang mit derartigen Produkten. Hersteller*innen sollten gerade bei der Speicherung der Daten große Sorgfalt an den Tag legen.

Grundsätzlich ist es wichtig, dass sich Käufer*innen schon vor dem Erwerb solcher Produkte über das anzuschaffende Gerät ausreichend informieren. Im Internet sind in der Regel alle Informationen dazu auf den Seiten seriöser Hersteller*innen abrufbar. Da es Unterschiede bei der Menge und Art der Datenverarbeitung zwischen den Herstellern gibt, lohnt es sich, im Vorfeld zu recherchieren, wenn man etwa vermeiden möchte, dass Daten aus dem eigenen Haushalt in ein Land außerhalb der EU oder dem Europäischen Wirtschaftsraum (sog. „Drittland") verschickt werden, wo Daten unter Umständen weniger gut geschützt sind.

Auch in der jeweiligen Datenschutzerklärung zu den Produkten sind die Datenverarbeitungen grundsätzlich beschrieben, so dass Kund*innen eine informierte Entscheidung treffen können. Dabei sollte darauf geachtet werden, dass möglichst Produkte ausgewählt werden, bei denen die Daten gut geschützt sind. Denn durch die grundsätzlich mögliche Option, smarte Geräte und Systeme auch aus der Ferne steuern zu können, werden diese anfälliger für unberechtigte Zugriffe durch Dritte. Dritte Personen könnten beispielsweise von außerhalb auf das Babyphone zugreifen und so Gespräche oder Videoaufnahmen abgreifen.

Aus rechtlicher Sicht gilt: Für die Erhebung der Daten zur Nutzung der smarten Produkte wird auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe b DS-GVO zurückgegriffen. Danach ist die Datenverarbeitung rechtmäßig, weil ohne sie die Hersteller*innen ihren Vertrag mit den Nutzer*innen nicht erfüllen könnten.

Erhoben werden dabei vielfältigste Daten. So wird für die Nutzung der smarten Funktionen in vielen Fällen zusätzlich zum Gerät auch ein persönlicher Account benötigt, mit dem sich die Kund*innen in der zugehörigen App einloggen können. Dazu werden meist mindestens die E-Mail-Adresse und ein Passwort abgefragt. Sollen über die App weitere Dienstleistungen wie die Wartung, der Kauf von Ersatzteilen etc. abgewickelt werden, sind in der Regel weitere Daten wie Name, Adresse, Telefonnummer, Geburtsdatum, Liefer- und Rechnungsadresse sowie Zahlungsdaten einzugeben. Im weiteren Verlauf können hier dann auch die Bestellhistorie und die gelieferten Produkte angezeigt werden. Für

die Einbindung der Geräte in die App, das sog. Pairing, sind bei manchen Hersteller*innen außerdem noch der Gerätetyp und die Seriennummer einzugeben. Zusätzlich werden die Kund*innen bei Verwendung der App möglicherweise gefragt, ob auch pseudonymisierte Geräte-Nutzungsdaten zu analytischen Zwecken erhoben werden dürfen.

Diese Einwilligung der Käufer*innen nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a, 7 DS-GVO wird oft direkt beim initialen Start der App eingeholt. Zudem wird im Rahmen der App-Einrichtung oft die Einwilligung für den Newsletter abgefragt. Wichtig für die rechtliche Wirksamkeit solcher Einwilligungen ist vor allem, dass sie freiwillig erfolgen und die relevanten Informationen vorab bereitgestellt werden, die notwendig sind, um die Verarbeitungsvorgänge zu verstehen, in die eingewilligt werden soll.

Ein weiteres Thema beim Einsatz smarter Geräte ist die Datenverarbeitung in Clouds. Für deren Rechtmäßigkeit muss der/die Gerätehersteller*in prüfen, ob der eingesetzte Cloud-Dienst hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen zum Schutz der Daten durchgeführt werden, etwa eine Verschlüsselung. Außerdem geht die Nutzung von smarten Produkten bisweilen mit Datenübermittlungen an Länder außerhalb des EWR einher (sog. Drittländer). Nicht selten setzen Hersteller*innen Clouddienste ein, die auf Speicherkapazitäten in Drittstaaten zurückgreifen. Wenn auf diesem Wege personenbezogene Daten gespeichert werden, müssen Hersteller*innen prüfen, ob für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission nach Kapitel V der DS-GVO vorliegt. Mit einem solchen Beschluss wird festgelegt, dass personenbezogene Daten in einem bestimmten Drittland einen mit dem europäischen Datenschutzrecht vergleichbaren adäquaten Schutz genießen. Existiert dieser nicht, muss der Hersteller mittels geeigneter Garantien ein angemessenes Schutzniveau garantieren. Käufer*innen sind zwar nicht verpflichtet, diese Voraussetzungen selbst zu prüfen. Dennoch ist es empfehlenswert, sich vor dem Kauf zu erkundigen, ob die Hersteller*innen personenbezogene Daten in „unsichere" Drittländer übermitteln und welche Schutzvorkehrungen für die Daten getroffen wurden. So können sie sich vergewissern, dass sie zum Beispiel ihre Betroffenenrechte weiterhin ausüben können, wenn es um die Drittlandsübermittlung geht.

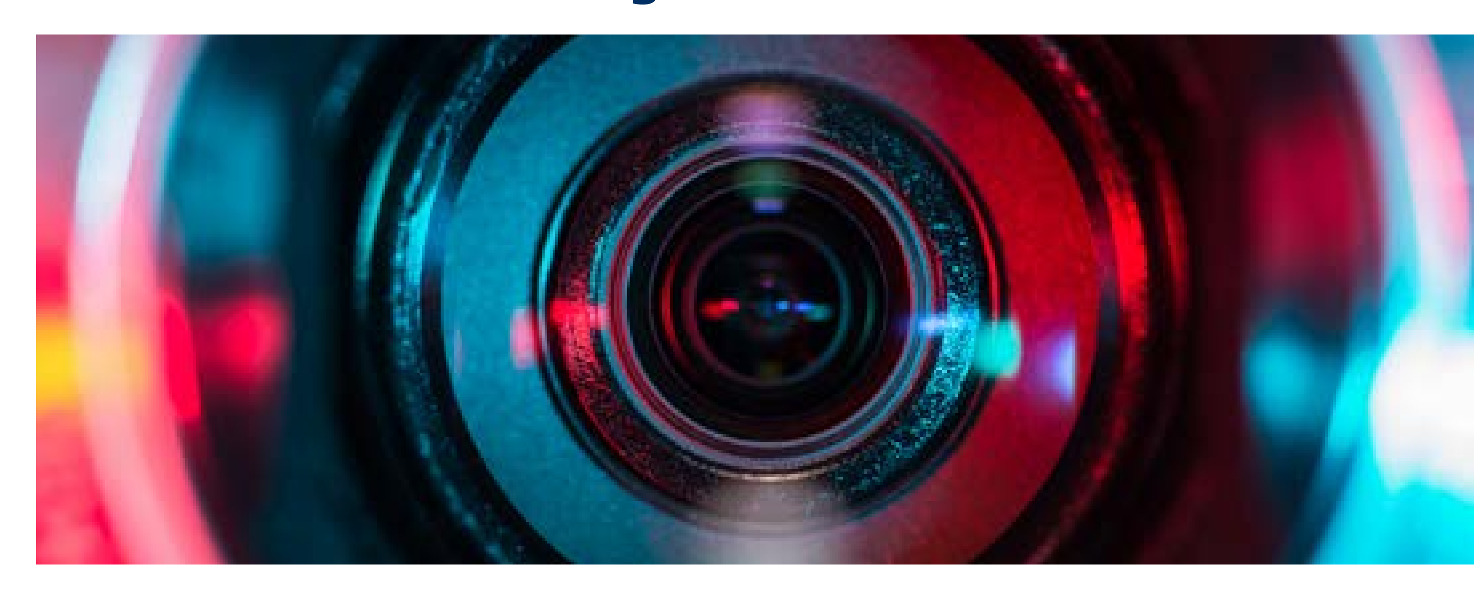
Den Hersteller*innen scheinen ihre Verpflichtungen allerdings durchaus bekannt. Aus Anlass einer konkreten Beschwerde hat die LDI NRW einen Produzenten von Smart Home-Geräten überprüft. Positiv konnte hierbei festgestellt werden, dass dem Thema Datenschutz und Vernetzung dort mit der gebotenen Sorgfalt begegnet wird. Der Großteil der Daten (Kundennummer, Land und E-Mail-Adresse) wird in einem Rechenzentrum in NRW aufbewahrt und nicht in einer externen Cloud, welche von

Drittanbietenden zur Verfügung gestellt wird. Außerdem ist es möglich, die Geräte dieses Herstellers weiterhin ohne die smarten Funktionen im herkömmlichen Sinne zu nutzen. Davon macht derzeit mehr als die Hälfte der Nutzer*innen auch Gebrauch.

Fazit

Die Gerätehersteller*innen sind verpflichtet, für einen datenschutzkonformen Einsatz ihrer smarten Haushaltsprodukte zu sorgen. Es ist zudem empfehlenswert, dass sich Käufer*innen vor der Anschaffung solcher Produkte über die Art der Datenverarbeitung, die damit einher geht, Gedanken machen und eine möglichst datensparsame Entscheidung treffen.

13. Videoüberwachung



13.1. Videoüberwachung im Außenbereich eines Museums? Ohne konkrete Gefährdung gibt es enge Grenzen

In Museen befinden sich oftmals Werke von hohem künstlerischem und wirtschaftlichem Wert. Das weckt Begehrlichkeiten bei Kriminellen. Aber rechtfertigt die abstrakte Sorge vor Diebstahl eine umfangreiche und langfristige Überwachung im öffentlich zugänglichen Außenbereich?

Kunstdiebstahl kann ein lukratives Geschäft sein, Museen beherbergen teilweise millionenschwere Kunstschätze. Nicht ohne Grund kommt es deshalb trotz hoher Sicherheitsvorkehrungen immer wieder zu spektakulären Diebstählen, etwa wie im Grünen Gewölbe in Dresden. Dass Museen dem mit noch mehr Überwachung begegnen wollen, ist verständlich. Doch wo verläuft die Grenze zwischen Schutz des Eigentums und Schutz der Privatsphäre von Passant*innen und Museumsbesucher*innen?

Die LDI NRW hat dies 2024 in einem Fall klären müssen, der ein privatrechtlich organisiertes Museum für moderne Kunst in einer Großstadt in NRW betrifft. Das Museum wollte aus Sicherheitsgründen die Speicherdauer der Videoüberwachung im Umfeld des Gebäudes, das sich in einem öffentlichen Park befindet, von drei Arbeitstagen auf 30 Tage erweitern. Dabei sollten nicht nur der unmittelbare Außenbereich videoüberwacht werden, sondern auch Teile des rund um die Uhr öffentlich zugänglichen Parks und teilweise umliegende Straßen und Häuser. Auf den entsprechenden Hinweisschildern informierte das Museum über die Speicherdauer nicht.

Die Überwachung des Museums war so ausgestaltet, dass Videoaufnahmen vom Sicherheitspersonal live mitverfolgt werden konnten. Was die Speicherung der Bilder anbelangt, hatte die Einrichtung gewisse Maßnahmen etabliert, die die Rechte Betroffener schonen sollten. So existiert etwa ein Blackbox-System mit der reversiblen Verpixelung von Personen. Das System ist nur im Verdachtsfall und zur Strafverfolgung durch zwei autorisierte Personen nach dem Vier-Augen-Prinzip einsehbar. Zugriffe werden protokolliert und erfolgen unter vorheriger Abstimmung mit dem Datenschutzbeauftragten des Museums.

Die Erweiterung der Speicherdauer auf 30 Tage rechtfertigten die Museumsverantwortlichen mit dem Wert der in dem Museum ausgestellten und gelagerten Güter und mit „kriminalistischer Erfahrung". Einbrüche und Diebstähle vor einigen Jahren in anderen Museen, vor allem in Berlin und Dresden, hätten gezeigt, dass in den Wochen vor der Begehung der Tat die Zielobjekte ausgespäht worden seien. Insofern bedürfe es einer längeren Speicherdauer von Bildern als bisher. Zudem habe eine Videoüberwachung mit langer Speicherdauer eine abschreckende Wirkung und habe letztendlich in einem der Fälle zur Aufklärung der Straftat wesentlich beigetragen.

Für die LDI NRW sind das keine überzeugenden Argumente für einen derart tiefgreifenden Eingriff in die Freiheitsrechte der Bürger*innen. Hinsichtlich der Videoüberwachung gilt, dass Bereiche außerhalb des unmittelbaren Kerns des Museums, also mitüberwachte Straßenräume und Teile der Parkanlage, in denen sich keine Kunstobjekte befinden, generell nicht überwacht werden dürfen. Die LDI NRW hat das Museum deshalb verpflichtet, den Kamerafokus entsprechend zu verändern.

Auch eine längere Speicherdauer konnte nicht gebilligt werden. In der Regel sind drei Arbeitstage für die hier verfolgten Zwecke ausreichend. Von dieser Speicherdauer geht auch eine Orientierungshilfe der DSK für vergleichbare Sachverhalte aus. Sie soll sicherstellen, dass das Datenschutzrecht in dieser Frage in ganz Deutschland einheitlich angewendet wird. Verantwortliche dürfen nur mit ausreichender Begründung von dieser Regelspeicherdauer abweichen. Die Argumentation des Museums, man müsse für den Fall eines späteren Einbruchs, zum Erkennen von Ausspähversuchen oder zur Abschreckung länger speichern, erfüllt diese Ausnahmevoraussetzung nicht.

Dabei fehlt es schon an der Geeignetheit der Maßnahme. Angenommen, das Museum würde vor einem Diebstahl wirklich ausgespäht, ist auch anzunehmen, dass die Videoüberwachung frühzeitig entdeckt und erkundet wird, welchen Bereich die Kameras erfassen. Das Ausspähen würde deshalb, jedenfalls bei professionell vorgehenden Einbrecher*innen, unbemerkt stattfinden oder so frühzeitig, dass es auch bei langer Speicherdauer nicht erfasst wäre. Aber selbst, wenn man die längere Speicherdauer für geeignet hielte, würde die Zulässigkeit der

längerfristigen Videoüberwachung an der Abwägung der gegenseitigen Interessen scheitern. Das Ermitteln aufklärungsrelevanter Tatsachen im öffentlichen Raum ist grundsätzlich Sache der Staatsanwaltschaft und nicht privater Einrichtungen. Das Interesse der Allgemeinheit, sich im öffentlichen Raum unbeobachtet zu bewegen, ist deshalb deutlich höher zu bewerten als das Interesse des Museums „mögliche Ausspähversuche" aufzuzeichnen, die nur befürchtet werden. Andernfalls würden alle Passant*innen und Besucher*innen, die in den letzten dreißig Tagen aufgezeichnet wurden, automatisch unter den Generalverdacht fallen, potentielle Ausspäher*innen zu sein. Es käme zu einer Speicherung auf Vorrat für einen Fall, von dem gänzlich ungewiss ist, ob er sich jemals ereignen wird.

Selbst die Polizei hat so weitreichende Befugnisse zur Beobachtung der Öffentlichkeit nicht, wie sie das Museum umsetzen möchte. Sie kann nur dort beobachten, wo tatsächlich regelmäßig Straftaten begangen werden. Bei allem Verständnis für den Schutz hochrangiger Kulturgüter müssen Museen deshalb auf andere Sicherheitsvorkehrungen verwiesen werden, die milder mit den Freiheitsrechten der Bürger*innen umgehen, wie etwa Alarmanlagen.

Die LDI NRW hat es bei dieser Güterabwägung aber nicht belassen. Wegen eines Hinweises des Museums auf die Praxis anderer Einrichtungen in Deutschland hat die LDI NRW zusätzlich die anderen Datenschutzaufsichtsbehörden in Deutschland nach ihren Erkenntnissen befragt. Dabei wurde nahezu durchgängig mitgeteilt, dass ähnliche Pläne von Museen oder Einrichtungen, die Güter von hohem Wert ausstellen oder lagern, nicht an sie herangetragen worden seien. Lediglich in einem Fall sei von einem Museum eine Speicherdauer von 30 Tagen angestrebt, aber deren Erforderlichkeit nicht belegt worden.

Im Ergebnis konnte auch das Museum in NRW nicht überzeugend begründen, warum die längere Speicherdauer erforderlich sei. Die „kriminalistische Erfahrung", die eine längere Speicherdauer rechtfertigen sollte, wurde nur abstrakt vorgetragen und konnte für den konkreten Fall nicht näher belegt werden. Hinweise auf zwei Einbrüche in anderen Städten und vage Befürchtungen reichen als Begründung allein nicht aus, um die Speicherdauer, wie gefordert, auf 30 Tage auszudehnen.

Darüber hinaus stoppte die LDI NRW auch das Vorhaben der Einrichtung, auf den vorgelagerten Hinweisschildern an den Zugangswegen die Speicherdauer zu verschweigen. Vielmehr sollte es dort heißen, die Speicherung erfolge „entsprechend der gesetzlichen Vorgaben" – allenfalls noch mit einem ein Zusatz versehen „Weitere Informationen erhalten Sie an der Kasse im Erdgeschoss".

Das Museum verschweigt zudem auf den vorgelagerten Hinweisschildern an den Zugangswegen die Speicherdauer; stattdessen heißt es nur, die

Speicherung erfolge „entsprechend der gesetzlichen Vorgaben" – und „Weitere Informationen erhalten Sie an der Kasse im Erdgeschoss".

Die LDI NRW bewertet auch dies als nicht mit der DS-GVO vereinbar. Danach müssen betroffene Personen bereits zum Zeitpunkt der Erhebung ihrer Daten die Informationen darüber erhalten, für welche Dauer ihre personenbezogenen Daten gespeichert werden. Falls dies nicht möglich ist, müssen wenigstens die Kriterien für die Festlegung dieser Dauer genannt werden. Da hier mit drei Arbeitstagen eine konkrete Regelspeicherdauer feststeht, ist diese also bereits auf den Hinweisschildern anzugeben. In Fällen, in denen Daten ausnahmsweise über die Regelspeicherfrist hinaus gespeichert werden dürfen, etwa um Sachbeschädigungen aufzuklären, kann dafür hingegen keine präzise Dauer mitgeteilt werden. Hier reicht es aus, wenn angegeben wird, dass bei aufgezeichneten Straftaten, so lange gespeichert werden darf, wie dies für die Rechtsverfolgung notwendig ist.

Das Museum wurde dementsprechend aufgefordert, die Hinweisbeschilderung im Umfeld des Museums den gesetzlichen Vorgaben anzupassen und hat dies zugesagt.

Fazit

Abstrakte Gefahren für Museen rechtfertigen in der Regel keine Abweichungen von den generellen Vorgaben des Datenschutzrechts. Dies gilt auch für das Ausmaß der überwachten Bereiche, die Regelspeicherdauer von drei Arbeitstagen und die Pflicht zur Angabe der konkreten Speicherdauer auf der Hinweisbeschilderung.

13.2. Keine ungeschwärzte Akteneinsicht, um Informant*innen zu enttarnen – Gericht stützt Haltung der LDI NRW



Die LDI NRW verrät grundsätzlich nicht, wer sich bei ihr über einen Datenschutzverstoß beschwert hat. Eine Geschäftsfrau wollte das nicht akzeptieren und bemühte ein Gericht, um den Namen derjenigen Person zu erfahren, die sich über ihre Videoüberwachung beschwert hatte. Das Gericht wurde deutlich.

Der Fall aus dem vergangenen Jahr steht exemplarisch für einen Konflikt, der mittlerweile häufig vorkommt: Immer öfter setzen Geschäftsleute zum Schutz ihrer Geschäftsräume auf Videoüberwachung. Dementsprechend wächst auch die Zahl der Beschwerden von Menschen, die nicht aufgenommen werden wollen.

Konkret hatte die Inhaberin eines Friseursalons ihren Geschäftsraum mit einem Kamerasystem ausgestattet, woraufhin eine Person bei der LDI NRW als zuständiger Datenschutzaufsichtsbehörde beschwerte. Die für die Videoüberwachung Verantwortliche wiederum beantragte als Reaktion darauf Akteneinsicht, um zu erfahren, wer denn genau mit ihrer Videoüberwachung nicht einverstanden war. Die LDI NRW erteilte der Verantwortlichen zwar Akteneinsicht, diese aber nur teilweise. Personenbezogene Daten der Person, die sich beschwert hatte, wurden vorher geschwärzt. Daraufhin erhob die Inhaberin des Salons Klage, weil sie auch Einsicht in die geschwärzten Angaben wollte.

Für die LDI NRW gilt in solchen Fällen: Daten von Personen, die sich bei der LDI NRW über einen Datenschutzverstoß beschwert haben, werden im Rahmen der Akteneinsicht grundsätzlich nicht bekannt gegeben. Ausnahmen hiervon werden nur in besonderen Fällen gemacht, beispielsweise, wenn Hinweisgeber*innen mit der Weitergabe ihrer Daten einverstanden sind.

Ihren Grund hat diese Haltung darin, dass der Gesetzgeber dem Schutz der Personen, die auf mögliche Datenschutzverstöße aufmerksam machen, eine herausgehobene Stellung zugewiesen hat. Das Datenschutzrecht ist so ausgestaltet, dass nach Art. 77 Abs. 1 DS-GVO jeder Mensch die Möglichkeit hat, sich an Datenschutzaufsichtsbehörden, wie die LDI NRW, mit dem Vorbringen zu wenden, bei der Verarbeitung personenbezogener Daten seien seine Rechte verletzt worden. Durch eine solche Anrufung dürfen der betroffenen Person aber keine Nachteile entstehen, wie aus § 29 Satz 2 des DSG NRW hervorgeht.

Mit dieser Regelung hat der Gesetzgeber folglich dem Schutz von Personen, die auf mögliche Datenschutzverstöße aufmerksam machen, eine herausgehobene Stellung zugewiesen. In Anbetracht dieses besonderen Schutzes, der auch ein öffentliches Interesse darstellt, können Auskünfte zu hinweisgebenden Personen nur in seltenen Ausnahmefällen erfolgen – nämlich dann, wenn gewichtige Gründe vorliegen, die die entgegenstehenden Interessen überwiegen. Dies ist meist nicht der Fall – und traf auch auf den konkreten Fall nicht zu. Das Interesse am Informant*innenschutz überwiegt nach Auffassung der LDI NRW in der Regel das Interesse an einer „ungeschwärzten" Akteneinsicht.

So hat es auch das Verwaltungsgericht gesehen, das die Verantwortliche angerufen hatte. Das Gericht wies die Klägerin im Laufe des Verfahrens darauf hin, dass ihre Klage auf ungeschwärzte Akteneinsicht mit dem Ziel, die Identität der hinweisgebenden Person zu erfahren, mit sehr hoher Wahrscheinlichkeit keinen Erfolg haben wird. Die Klägerin bestand zunächst trotzdem auf einer mündlichen Verhandlung. Kurz vor der mündlichen Verhandlung nahm sie dann die Klage zurück.

Fazit

Die deutlichen Hinweise des Verwaltungsgerichts bestätigen die Auffassung der LDI NRW, dass das Interesse an der Geheimhaltung der Person, die ihr Beschwerderecht wahrnimmt, in der Regel das Interesse des Verantwortlichen an der Kenntnis der Identität der hinweisgebenden Person überwiegt. Die Identität von Informant*innen muss deshalb regelmäßig – auch im Fall einer Akteneinsicht – nicht offenbart werden.

14. Datenschutz im Verein



14.1. Darf ein Verein ein erweitertes Führungszeugnis von Mitarbeiter*innen verlangen?

Arbeiten mit Kindern und Jugendlichen ist ein sensibles Thema – gerade auch im Verein. Deren Verantwortliche verlangen deshalb oft Einsicht in erweiterte Führungszeugnisse, etwa von ehrenamtlichen Fußballtrainer*innen oder auch Mitarbeiter*innen in Jugendorganisationen. Bei der LDI gehen immer wieder Anfragen dazu ein. Fest steht: Nicht immer ist der Wunsch auf Einsichtnahme berechtigt.

Nicht jedes Leben verläuft stets gradlinig und fehlerlos. Manche Menschen begehen Straftaten, landen teilweise sogar im Gefängnis – aber finden später auf den rechten Weg zurück. Bis dahin hat ihr Lebensweg allerdings Spuren hinterlassen, ob auf Papier oder elektronisch. Ihre Verfehlungen sind etwa im Bundeszentralregister gelandet, und können von da aus auch in ein erweitertes Führungszeugnis eingehen.

Was aber von diesen personenbezogenen Daten geht andere noch an? Welche Informationen des einst weniger tadellosem Lebens dürfen in die Hände eines Vereins gelangen, bei dem sich die betroffene Person für ein Ehrenamt bewirbt, und dort eingesehen werden? Immer wieder ist es auch 2024 vorgekommen, dass sich Vereine und ehrenamtliche Betreuer*innen dazu bei der LDI NRW erkundigt haben. Tatsächlich ist es für alle Beteiligten von großer Bedeutung, die Rechtslage genau zu kennen.

Grundsätzlich erlaubt die DS-GVO in Art 10 Satz 1, 2. Halbsatz den EU-Mitgliedsstaaten, ein Gesetz zu erlassen, mit dem die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und

Straftaten oder damit zusammenhängende Sicherungsmaßregeln zugelassen wird. Der deutsche Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht. In § 72a SGB VIII ist geregelt, dass Träger der öffentlichen Jugendhilfe für die Wahrnehmung ihrer Aufgaben in der Kinder- und Jugendhilfe keine Personen beschäftigen oder vermitteln dürfen, welche rechtskräftig wegen bestimmter Straftaten verurteilt wurden. Hierbei handelt es sich vor allem um Straftatbestände im Zusammenhang mit der Verletzung von Schutz- und Fürsorgepflichten sowie um Sexualstraftaten.

Die Träger der öffentlichen Jugendhilfe sollen darüber hinaus durch Vereinbarungen insbesondere mit den Trägern der freien Jugendhilfe sicherstellen, dass auch bei den freien Trägern eine entsprechende Überprüfung von Personen erfolgt, die mit Kindern und Jugendlichen umgehen. Zu den Trägern der freien Jugendhilfe zählen auch mit Jugendhilfemitteln geförderte Vereine. In den Bescheiden über die Fördermittel werden diese Vereine regelmäßig dazu verpflichtet, ihr Personal nach den obigen Bestimmungen zu überprüfen.

Aber darf dazu von den potenziellen Mitarbeiter*innen auch ein erweitertes Führungszeugnis angefordert werden? Das erweiterte Führungszeugnis enthält gegenüber dem normalen Führungszeugnis zusätzlich Verurteilungen wegen Sexualdelikten, die für die Aufnahme in das einfache Zeugnis zu geringfügig sind, wie zum Beispiel Erstverurteilungen zu geringfügigen Strafen.

Öffentliche Träger der Jugendhilfe, kreisfreie Städte oder Kreise, die zum Beispiel Kinderheime betreiben, sind bereits nach § 72 Abs. 3 SGB VIII verpflichtet, Personal zu überprüfen, das in solchen Einrichtungen eingesetzt wird. Die datenschutzrechtliche Erlaubnis, dafür ein erweitertes Führungszeugnis anzufordern, folgt unmittelbar aus der DS-GVO, die in Art. 6 Abs. 1 Unterabsatz 1 Buchstabe c die Verarbeitung personenbezogener Daten zulässt, sofern dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

In den anderen Fällen, insbesondere bei der freien Jugendhilfe, kommt Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f der DS-GVO zum Einsatz. Die Vorschrift verlangt eine Interessenabwägung zwischen den Rechten desjenigen, der Daten verarbeitet und desjenigen, den sie betreffen. Träger der freien Jugendhilfe haben ein berechtigtes Interesse, ein erweitertes Führungszeugnis anzufordern – auch weil sie andernfalls wohl keine öffentlichen Mittel zur Durchführung ihrer Aufgaben erhalten würden. Außerdem liegt die Anforderung auch im berechtigten Interesse der Kinder und Jugendlichen, die im Verein bereut werden.

Die notwendige Abwägung mit den Interessen der Betroffenen, die das Führungszeugnis vorlegen sollen, ist im Wesentlichen bereits durch § 72a SGB VIII gesetzlich vorgegeben. Insofern kommt es für die Fra-

ge, ob ein erweitertes Führungszeugnis im Einzelfall verlangt werden kann, darauf an, ob die Voraussetzungen dieser Vorschrift vorliegen. Danach müssen die Vereine identifizieren, welche bei ihnen eingesetzten Personen Aufgaben der Jugendhilfe wahrnehmen und Kinder oder Jugendliche beaufsichtigen, betreuen, erziehen oder ausbilden oder einen vergleichbaren Kontakt haben. Dazu gehören in jedem Fall leitende Betreuungspersonen. Ob auch Personen, die „einen vergleichbaren Kontakt” haben, der Regelung unterfallen, hängt hingegen von der konkreten Ausgestaltung der Organisation und dem Einzelfall ab.

Weiter kommt es auf die Art des Kontakts an. Entscheidend sind hier Faktoren, die ein Gefahrenpotenzial beinhalten, das ein besonderes Vertrauensverhältnis missbraucht werden könnte, zum Beispiel eine große Altersdifferenz oder ein Macht-/Hierarchieverhältnis zwischen Betreuer*in und Kind. Zu beachten ist außerdem das Alter der von der Abfrage betroffenen Person. Führungszeugnisse können zwar ab Strafmündigkeit verlangt werden, dass heißt ab Vollendung des 14. Lebensjahrs. Jedoch muss in jedem Einzelfall die Erforderlichkeit und Sachdienlichkeit genau geprüft werden.

Sofern die Vorlage eines erweiterten Führungszeugnisses verlangt wird, muss die betroffene Person dieses beim Bundeszentralregister beantragen und selbst dem Träger der Jugendhilfe zur Einsicht vorlegen. Wichtig ist allerdings: Der Träger darf das Zeugnis nicht aufbewahren – auch nicht in abgeschlossenen Schränken. Über die eingesehenen Daten darf nach § 72a Abs. 5 SGB VIII nur folgendes gespeichert werden: der Umstand der Einsichtnahme selbst, das Datum des Führungszeugnisses und die Information, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach § 72 Abs. 1 Satz 1 SGB VIII oder einer anderen Straftat rechtskräftig verurteilt wurde, die die Person als ungeeignet im Umgang mit Kindern und Jugendlichen erscheinen lässt.

Außerdem darf der Verein die gespeicherten Daten nur verarbeiten, soweit dies erforderlich ist, um die Eignung für eine spezifische Tätigkeit zu prüfen. Er darf diese Informationen also keinesfalls an Dritte weitergeben. Die Daten sind zudem vor dem Zugriff Unbefugter zu schützen und spätestens sechs Monate nach der letztmaligen Ausübung einer Tätigkeit zu löschen, für die die Einsicht erforderlich war.

Fazit

Vereine, die in der freien Jugendhilfe mitwirken, dürfen von den Personen, die Kinder und Jugendliche betreuen sollen, in vielen Fällen die Vorlage erweiterter Führungszeugnisse verlangen. Das gilt sowohl für haupt- als auch für ehrenamtlich tätige Personen. Eine Aufbewahrung von erweiterten Führungszeugnissen ist allerdings unzulässig. Bestimmte im Gesetz festgelegte Daten dürfen hingegen sechs Monate gespeichert werden.

14.2. Datenschutz im Kleingarten: Vorsicht beim öffentlichen Aushängen von Protokollen

Menschen suchen in ihrer Gartenlaube Ruhe und Erholung. Umso wichtiger ist es, dass es in Schrebergartensiedlungen klare Regeln gibt, die alle kennen und an die sich alle halten – auch in Sachen Datenschutz. Besondere Rücksichtnahme gilt, wenn Papieraushänge ins Spiel kommen.

Deutschland lebt vom Vereinswesen. Allein der Bundesverband der Kleingartenvereine Deutschlands e.V. zählt knapp 900.000 Kleingärtner*innen, die unter seinem Dach organisiert sind. Da bleibt es nicht aus, dass es auch mal zu Streitigkeiten kommt. Fragen der Bepflanzung gehören dabei ebenso dazu wie Unstimmigkeiten beim Datenschutz. So auch in einem Fall aus dem vergangenen Jahr, der die LDI NRW beschäftigt hat.

Eine Person hatte sich darüber beschwert, dass in einem Kleingartenverein das Protokoll der Jahreshauptversammlung zur Einsichtnahme ausgehängt worden war, und zwar in einem Schaukasten des Vereinsheims, der an einem öffentlichen Weg liegt. In dem Protokoll waren auch verschiedene Anträge nachzulesen mitsamt den Namen der Antragssteller*innen.

Die LDI NRW musste den Verein deswegen verwarnen. Für eine Offenlegung von personenbezogenen Daten an jeden, der des Weges kommt, fehlte es an einer Rechtsgrundlage. Der Wunsch des Vereins, den traditionellen Weg des Aushangs zu wählen, muss hinter dem Interesse des einzelnen Mitglieds an Privatheit zurückstehen – zumal auch keine Einwilligung des Mitglieds vorlag, das die Beschwerde bei uns einreichte.

Als Rechtsgrundlage für den Aushang kommt auch nicht Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f der DS-GVO in Betracht. Bei der Abwägung der sich gegenüberstehenden Interessen überwiegen die Interessen der betroffenen Person am Schutz ihrer personenbezogenen Daten das grundsätzlich berechtigte Interesse des Vereins, Dritte über einen Aushang zu informieren.

Dabei ist zu berücksichtigen, dass der öffentliche Aushang dazu führt, dass alle am Gelände vorbeispazierenden Personen aus dem Protokoll erfahren, dass die dort namentlich Genannten zu den Kleingartenbesitzer*innen gehören. Nicht jeder aber möchte von ungebetenen Besucher*innen überrascht werden, die ihn aufgrund des Protokolls spontan aufsuchen. Schließlich ist der Kleingarten für viele Mitglieder auch ein Rückzugsraum. Es gibt heutzutage außerdem andere, einfache Wege, ein Protokoll der Mitgliederversammlung bekannt zu geben.

Für den Verein war die Rechtslage letztendlich nachvollziehbar. Er hat angekündigt, künftig keine Protokolle mehr offen auszuhängen.

Fazit

Vereine, die Sitzungsprotokolle einem offenen Personenkreis ohne Einwilligung der dort genannten Personen zugänglich machen möchten, sollten die personenbezogenen Daten in den Protokollen vor der Veröffentlichung unkenntlich machen bzw. schwärzen. Für weitere Informationen hält die LDI NRW auf ihrer Website für Vereine die Broschüre „Datenschutz im Verein" bereit, die viele wichtige Bausteine für einen gelingenden Datenschutz im Verein enthält.

15. Zahlen und Fakten



Eingabesituation im Überblick

Im Jahr 2024 haben uns insgesamt **12.490 Eingaben** erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen.

Grundsätzlich nicht erfasst haben wir die zahlreichen telefonischen Anfragen.

Im Jahr 2023 waren es 11.050, 2022 waren es rund 10.500 und 2021 11.900 schriftliche Eingaben.

Von den Eingaben waren

7.539 **Beschwerden** nach Art. 77 DS-GVO,

759 **Hinweise von Dritten,**

893 **schriftliche Beratungsanfragen,**

28 **Begleitungen bei Rechtsetzungsvorhaben,**

3 **Genehmigungsverfahren,**

2.170 **Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen und

429 **Eingaben ohne Kategorie.**

Beschwerden und Beratungsanfragen

Im Jahr 2024 haben uns **7.539 Beschwerden** erreicht.

Eine Beschwerde liegt nach Art. 77 DS-GVO vor, wenn eine Person vorträgt, dass ein sie persönlich verletzender Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt.

Eingaben, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind, können wir von Amts wegen aufgreifen. Solche **Hinweise von Dritten** haben wir **759 Mal** erhalten.

Schriftliche **Beratungsanfragen** haben wir **819** erhalten, sowohl von Verantwortlichen und Auftragsverarbeitern als auch von betroffenen Personen.

Meldungen von Datenschutzverletzungen

Meldungen nach Art. 33 DS-GVO zu sog. Datenpannen haben uns **2.170 Mal** erreicht.

Im Jahr 2023 waren es 2.039, 2022 waren es 1.829 Meldungen und 2021 waren es 1.841 Meldungen.

Eine Verletzung des Schutzes personenbezogener Daten, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss der Verantwortliche unverzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde melden (Art. 33 DS-GVO).

Thematisch Zuordnung der gemeldeten Datenpannen:

30 Prozent Cyberangriffe

26 Prozent Fehlversand

18 Prozent andere unbefugte Weitergabe: 18 Prozent

4 Prozent offene E-Mailverteiler

4 Prozent Einbruch/Diebstahl: 4 Prozent

4 Prozent anderer Verlust von Dokumenten oder Speichermedien

3 Prozent unbefugte Veröffentlichung: 3 Prozent

11 Prozent Sonstiges

Abhilfemaßnahmen

Um eine Überwachung und Durchsetzung der DS-GVO sicherzustellen, werden den Aufsichtsbehörden in Art. 58 Abs. 2 DS-GVO einheitliche eingeräumt.

Bußgeldverfahren

Als Maßnahme nach **Art. 58 Abs. 2 Buchstabe i** wurden bei der Zentralen Bußgeldstelle der LDI NRW **64 Bußgeldverfahren eingeleitet** bzw. zur weiteren Verfolgung von den Staatsanwaltschaften übernommen.

24 Bußgeldbescheide wurden erlassen und **62 Verfahren wurden durch Rechtskraft, Einstellung oder Gerichtsentscheidungen abgeschlossen.** Das **höchste Bußgeld** betrug **25.000 Euro,** der **Mittelwert** aller Bußgelder **2.292 Euro** und der **Median 875 Euro.**

Weitere Abhilfemaßnahmen

Von den weiteren in Art. 58. Abs. 2 DS-GVO genannten Abhilfemaßnahmen hat die LDI NRW die folgenden Maßnahmen ergriffen:

1.367 **Hinweise** nach Art. 58 Abs. 1 d),

1 **Warnung** nach Art. 58 Abs. 2 a),

31 **Verwarnungen** nach Art. 58 Abs. 2 b),

153 **Anweisungen** nach Art. 58 Abs. 2 d),

1 **Beschränkung** nach Art. 58 Abs. 2 f).

Davon erfasst sind Verfahren, die bereits in den Vorjahren eingeleitet wurden, während viele im Jahr 2024 begonnene Verfahren noch nicht beendet und nicht erfasst sind. Oft sind die Verfahren sowohl in zeitlicher als auch in rechtlicher Hinsicht aufwendig. Nicht selten bedarf es vieler Kontakte und eines umfangreichen Schriftwechsels, bis es am Ende zu einer Abhilfemaßnahme etwa in Form eines Bußgeldbescheides kommt. Zudem setzt die LDI NRW im Kontakt mit den Verantwortlichen nach wie vor den Schwerpunkt auf Beratung und Sensibilisierung. Häufig werden so ohne eine förmliche Abhilfemaßnahme einvernehmliche, konstruktive Lösungen gefunden, die nicht nur den Einzelfall datenschutzgerecht lösen, sondern auch für die zukünftige Praxis der Verantwortlichen und Auftragsverarbeiter einen Gewinn für den Datenschutz bedeuten.

Europäische Verfahren

Die DS-GVO sieht Verfahren für eine europäische Meinungsbildung und Entscheidungsfindung der Datenschutzaufsichtsbehörden vor. Das einheitliche europäische Recht soll in den Mitgliedstaaten auch einheitlich angewendet werden. Da die Regelungen der DS-GVO oft allgemein gehalten sind, haben die Aufsichtsbehörden die Aufgabe, das neue Recht in der Interpretation und in der Praxis zu harmonisieren. Dazu müssen sich die Behörden abstimmen und – teils verbindliche – Rechtsauffassungen entwickeln. Die Meinungsbildung der europäischen Aufsichtsbehörden findet in Abstimmungsverfahren der Behörden untereinander und im EDSA statt.

Für viele Abstimmungsprozesse wird das Binnenmarkt-Informationssystem (Internal Market Information System, abgekürzt IMI) als IT-Plattform eingesetzt. Die Plattform IMI unterstützt die Verfahren der Zusammenarbeit und Kohärenz über komplexe Module. Wird ein Modul in IMI gestartet, generiert das System eine automatische Benachrichtigung, die bei der empfangenden Behörde bearbeitet werden muss. Arbeitssprache in IMI ist Englisch.

Unter anderem tauschen sich die betroffenen Aufsichtsbehörden über grenzüberschreitende Fälle aus und stimmen Entscheidungen ab. Geht beispielsweise bei uns eine Beschwerde in Bezug auf eine grenzüberschreitende Datenverarbeitung ein, leiten wir als Eingangsbehörde die ersten notwendigen Schritte über IMI in die Wege. Geht über IMI eine Meldung über eine grenzüberschreitende Datenverarbeitung ein, prüfen wir, ob wir europaweit federführend sind oder uns als betroffene Behörde an den weiteren Verfahrensschritten beteiligen.

Im Jahr 2024 war die LDI NRW in **2.272 Fällen** mit gestarteten IMI-Modulen befasst. Im Jahr 2023 waren es 2.182 Fälle, 2022 waren es 1.721 Fälle und im Jahr 2021 1.558 Fälle.

Wir hatten bei **zehn** europäischen Verfahren die **Federführung,** bei **65** Verfahren waren wir in unserer **Zuständigkeit betroffen** und in **14** Verfahren nach Art. 60 ff. DS-GVO (**Zusammenarbeit oder Kohärenzverfahren**) beteiligt.

Förmliche Begleitung bei Rechtsetzungsvorhaben

Im Jahr 2024 wurde die LDI NRW bei mehreren Rechtsetzungsvorhaben beteiligt.

Die LDI NRW ist frühzeitig über Entwürfe für Rechts- und Verwaltungsvorschriften zu unterrichten, wenn diese eine Verarbeitung personenbezogener Daten vorsehen (vgl. § 27 Abs. 5 Satz 2, § 57 Abs. 5 DSG NRW).

Wir wurden in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren beteiligt. Nicht alle Verfahren hatten dabei einen datenschutzrechtlichen Bezug, so dass wir dazu keine inhaltliche Stellungnahme abgegeben haben.

Gesetz zur Novellierung der Verschlusssachenanweisung NRW

- Gesetzes zur Novellierung der Gefangenenvergütung in den Landesjustizvollzugsgesetzen
- 7. Verordnung zur Änderung der Verordnung über die Zuständigkeiten nach dem Berufsbildungsgesetz (BBiGZustVO)
- Gesetz zur Änderung des Ausführungsgesetzes NRW Glücksspielstaatsvertrag
- Verordnung zur elektronischen Durchführung der öffentlichen Wohnraumförderung nach dem Gesetz zur Förderung und Nutzung von Wohnraum für das Land Nordrhein-Westfalen mit dem Fachverfahren WohnWeb (VO WohnWeb)
- Gesetz zur Änderung kommunalrechtlicher und weiterer Vorschriften im Land NRW
- Gesetz zur Änderung verwaltungsverfahrensrechtlicher, verwaltungsvollstreckungsrechtlicher und kostenrechtlicher Vorschriften
- Gesetz zur Verarbeitung von personenbezogenen Daten zum Schutz der Beschäftigten öffentlicher Stellen vor gefährdenden Personen
- Verordnung über den Betrieb von Forschungsinformationssystemen
- Gesetz zur Änderung des ArchivG NRW
- Gesetz zur Modernisierung des Sparkassenrechts und zur Änderung weiterer Gesetze
- Gesetzes über die Errichtung des Landesamtes für Gesundheit und Arbeitsschutz NRW sowie zur Änderung des Gesetzes über den öffentlichen Gesundheitsdienst (LFGA und ÖGD)
- Novellierung des Rettungsgesetzes NRW
- Gesetz zur Änderung des Gesetzes zur Ausführung des Asylbewerberleistungsgesetzes (2. AG AsylbLG)

- Referentenentwurf Registerzensusgesetz (RegZensG); Länderbeteiligung
- Gesetz zur Änderung des Statistikgesetzes NRW
- Gesetz zur Regelung einer Landesstatistik über die Ausbildungen und Weiterbildungen im Bereich der Gesundheitsfachberufe und zur Änderung des Landesausführungsgesetzes Pflegeberufe (GBAStatG)
- BDSG-Novelle
- Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679
- Gesetz zur Änderung des Hochschulgesetzes

Transparenz

Diese und weitere Informationen sind unter
www.ldi.nrw.de/zahlen-und-daten veröffentlicht.

2. Teil: Informationsfreiheitsbericht



1. Vorwort

Nur alle zwei Jahre berichten wir auch zur Informationsfreiheit. Deshalb ist sie aber nicht weniger wichtig. Im Gegenteil: Das Bedürfnis der Bürger*innen nach einem transparenten Staat, nach transparenter Verwaltung, ist groß. Das zeigen die veröffentlichten Reaktionen auf jüngst bekannt gewordene Pläne, das Informationsfreiheitsgesetz (IFG) des Bundes abzuschaffen.

Und auch auf Landesebene ist es immer wieder wichtig, dieses Bedürfnis zu betonen. Die Landesregierung hatte 2022 durch ihre im Koalitionsvertrag festgehaltenen Ziele die Hoffnung geweckt, dass das IFG des Landes um weitere Elemente zu mehr Transparenz angereichert würde. Zumindest sollte die Weiterentwicklung des Gesetzes mit Blick auf mögliche proaktive Veröffentlichung von Informationen geprüft werden. Zu dieser Prüfung sind mir bisher keine Ergebnisse bekannt.

Ich hoffe, dass dies nicht versandet. Aktiv Informationen der Verwaltung zu veröffentlichen, wie dies in modernen Transparenzgesetzen einzelner Länder und schon seit langem in transparenzfreundlichen skandinavischen Staaten üblich ist, ist aus meiner Sicht eine Chance. Es ist eine Chance für die Verwaltung, durch Fakten für die eigene Arbeit zu werben, eine Chance, Bürokratievorwürfe abzubauen und offene Informationspolitik zu betreiben, und nicht zuletzt auch eine Chance, um Fake News zu widerlegen. Letztendlich ist es ein Ausdruck von bürgerorientierter Arbeit und stärkt die Demokratie, wenn die Verwaltung die Grundlagen ihres Handelns von sich aus transparent macht. Daran möchte ich die Landesregierung an dieser Stelle noch einmal ausdrücklich erinnern.

Hinzu kommt, dass wir immer wieder auf Fälle stoßen, die eine Unsicherheit einzelner Behörden im Umgang mit dem IFG NRW belegen.

Gebührenberechnung, Geschäftsgeheimnisse oder der Schutz von Willensbildungsprozessen gehören in diese Kategorie. Besonders, wenn es um die Herausgabe von Verträgen oder Gutachten geht, über die die Verwaltung verfügt, ist es nicht im Interesse der Allgemeinheit, wenn Verwaltungen den Schutz des Meinungsbildungsprozesses oder eines Geschäftsgeheimnisses falsch einschätzen und Informationsansprüche ablehnen. Hier wollen die Bürger*innen oft einfach wissen, was mit Steuermitteln finanziert wird oder auf welche Erkenntnisse eine Verwaltung Entscheidungen stützt, die Auswirkungen für sie haben. Gerade grundlegende Verträge und Gutachten, über die die Verwaltung verfügt, sind oft von allgemeinem Interesse und sollten nicht nur auf Anfrage nach dem IFG herausgegeben werden, sondern können auch aktiv in einem Transparenzportal zur Verfügung gestellt werden.

In diesem Jahr ist es mir außerdem wichtig, auf die Entwicklung in der Rechtsprechung in den zurückliegenden zwei Jahren hinzuweisen. Wir sprechen in unserem Rechtsprechungsüberblick und auch in zwei Beiträgen einige bemerkenswerte Fälle im Berichtszeitraum an. Etwas enttäuschend dagegen war die im Berichtszeitraum beschlossene Änderung zur Modernisierung des Sparkassenrechts, die auch zu einer Änderung des IFG in Bezug auf kundenbezogene Daten öffentlicher Kreditinstitute führte. Kurz gesagt: Vergleichsweise versteckt findet sich in dem Gesetz eine Änderung, die es öffentlich-rechtlichen Kreditinstituten künftig erlaubt, Informationen zu verweigern, wenn es um die Verwendung öffentlicher Gelder geht. Der Bericht wird darauf näher eingehen. Aus unserer Aufsichtspraxis sind uns jedenfalls keinerlei Probleme mit IFG-Anträgen bekannt, die darauf abzielen würden, Informationen unmittelbar zu Daten von Kund*innen öffentlicher Kreditinstitute zu erhalten. Diese sind durch das IFG hinreichend geschützt. Die Änderung zielte damit offenbar auf ein faktisch nicht bestehendes Problem, beschneidet aber möglicherweise aufgrund unklarer Begriffe im Gesetz berechtigte Informationsinteressen der Öffentlichkeit.

Unabhängig von einer gesetzlichen Verpflichtung oder Weiterentwicklung des IFG sollte die Verwaltung die Chance einer proaktiven Informationspolitik jetzt schon aktiv nutzen und herausgabefähige Unterlagen veröffentlichen. Das macht die Bearbeitung von Einzelanfragen obsolet und stärkt die Demokratie.

Bettina Gayk
Frühjahr 2025

2. Informationsfreiheit in Deutschland

Die Beauftragten für Akteneinsicht, Informationsfreiheit und Transparenz des Bundes und der Länder haben sich zur Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) zusammengeschlossen. Ihr Ziel ist es, das Recht auf Informationszugang zu fördern und fortzuentwickeln. Mit Entschließungen, Positionspapieren und Stellungnahmen wendet sich die IFK dazu an verschiedene Adressat*innen, um Themen der Informationsfreiheit und der Transparenz voranzubringen. Der Vorsitz wechselt jährlich. Im Jahr 2023 hatte der damalige BfDI und im Jahr 2024 die sächsische Beauftragte den Vorsitz inne. Die IFK tagt in der Regel zweimal im Jahr. Die Sitzungen und Entschließungen werden vom Arbeitskreis Informationsfreiheit (AKIF) vorbereitet.

Entschließungen der IFK

Die Entschließungen der IFK tragen dazu bei, Optimierungspotentiale in Sachen Informationsfreiheit und/oder Transparenz öffentlich zu machen.

Die Entschließungen der Jahre 2023 und 2024 sind im Anhang abgedruckt und mit weiteren Informationen unter www.ldi.nrw.de/informationsfreiheit abrufbar. Auf drei der insgesamt acht Entschließungen möchten wir ein besonderes Augenmerk lenken:

- 25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz!

  Im Fokus dieser Entschließung steht die Forderung nach einer gesetzlichen Verpflichtung zur Unterrichtung der Öffentlichkeit über Umweltinformationen. Zwar gibt es bereits jetzt eine allgemeine Pflicht zur „Unterrichtung der Öffentlichkeit“, jedoch in den allermeisten Ländern (darunter NRW) und auf Bundesebene keinen entsprechenden einklagbaren Anspruch für jedermann. In diesem Zusammenhang sei noch einmal angemerkt, dass es in NRW auch noch immer an einer gesetzlichen Kontrollkompetenz für das Umweltinformationsgesetz NRW (UIG NRW) mangelt. Zunehmend werden wir zu UIG-Anliegen konsultiert. Wir benötigen für die Vermittlung in diesen Angelegenheiten ein offizielles Mandat. Hier ist der Gesetzgeber gefordert.

- **Pflicht zur Informationsfreiheit und Transparenz auch für Kommunen in Hessen und Sachsen!**

Die Gesetze in Hessen und Sachsen überlassen es ihren Kommunen, ob und inwieweit sie Informationen preisgeben wollen – freiwillig machen es bisher nur wenige. Dieses Defizit gibt es in NRW nicht. Hier waren die Kommunen von Beginn an vom Anwendungsbereich des IFG NRW erfasst. Trotz anfänglicher Vorbehalte hat sich das Gesetz bewährt, und sowohl Antragstellende als auch Verwaltung sind mittlerweile überwiegend routiniert im Umgang mit dem Gesetz. Wichtig ist die Anwendung im kommunalen Bereich vor allem deshalb, da das Geschehen vor der eigenen Haustüre für die Bürger*innen von besonderem Interesse ist.

In Sachen Transparenz – also aktiver Informationspolitik der Verwaltungen – sind wir nach wie vor nicht gut aufgestellt und belegen einen hinteren Platz in Vergleich zu anderen Ländern. Schlusslichter bei Transparenz und Informationsfreiheit bleiben aber weiterhin die Länder Niedersachen und Bayern, in denen es noch gar keine entsprechenden Gesetze gibt.

- **Gleicher Auftrag – gleicher Informationsanspruch gegenüber öffentlich-rechtlichen Rundfunkanstalten!**

Diese Entschließung fordert bundesweit einheitlich hohe Standards für den Anspruch auf Informationszugang gegenüber öffentlich-rechtlichen Rundfunkanstalten. In Ländern mit Mehrländeranstalten scheitert ein wirksamer Informationszugangsanspruch häufig an dem Erfordernis, dass dieser staatsvertraglich geregelt sein muss und eine entsprechende Regelung fehlt. In NRW stellt dies hingegen kein Problem dar. Nach § 55a des Gesetzes über den „Westdeutschen Rundfunk Köln” findet das IFG NRW auf den WDR Anwendung, „es sei denn, dass journalistisch-redaktionelle Informationen oder Ergebnisse der Prüfung des Landesrechnungshofs oder des sonst zuständigen Rechnungshofs nach § 46 [des Gesetzes] betroffen sind.

3. Diese Gerichtsentscheidungen zum Informationsfreiheitsrecht sollten Bürger*innen und Behörden kennen



3.1. IFG NRW kann im Einzelfall auch Zugang zu Verschlusssachen gewähren

Auch wenn Unterlagen formal als „VS-NUR FÜR DEN DIENSTGEBRAUCH" eingestuft sind, kann ein Anspruch auf Informationszugang nach dem IFG NRW bestehen. Dies hat das Verwaltungsgericht Düsseldorf in Bezug auf eine Dienstanweisung für Taser entschieden (Urteil vom 24. August 2023, **Az. 29 K 5628/21**). Das Gericht hat damit klargestellt, dass es für die Versagung des Zugangsanspruchs allein darauf ankommt, ob ein im IFG NRW normierter Ausschlussgrund vorliegt. Zwar genüge nach § 6 Satz 1 Buchstabe a IFG NRW bereits eine einfache Beeinträchtigung der öffentlichen Sicherheit, um den Anspruch auf Information zu verneinen. Die Behörde müsse aber Tatsachen vorbringen, aus denen sich plausibel nachteilige Auswirkungen ergeben können. Weil mit Blick auf die Tasernutzung bereits Einsatzkonzepte und weitreichende Details anderweitig veröffentlicht waren, konnte die Behörde nicht nachweisen, dass der Informationszugang das polizeiliche Handeln beeinträchtigt.

Auf Bundesebene gibt es – anders als in NRW – einen Ausschlussgrund, der direkt auf die Einstufung als Verschlusssachen abstellt (§ 3 Nr. 4 IFG Bund). Dort ist aber im Falle eines IFG-Antrags zu prüfen, ob die Einstufung auch materiell richtig ist, also die Voraussetzungen für die Geheimhaltung erfüllt sind.

3.2. Studierende haben Informationsanspruch auch in Bezug auf Prüfungszulassungen

Forschungseinrichtungen, Hochschulen und Prüfungseinrichtungen sind gemäß § 2 Abs. 3 IFG NRW nur informationspflichtig, soweit sie nicht im Bereich von Forschung, Lehre, Leistungsbeurteilungen und Prüfungen tätig werden. In Bezug auf Informationen zur Prüfungszulassung sind diese Stellen jedoch auskunftsverpflichtet, wie das Verwaltungsgericht Arnsberg entschieden hat (Urteil vom 6. März 2024, **Az. 7 K 652/22**): „Die Zulassung zu Prüfungen ist keine Tätigkeit „im Bereich von Prüfungen" im Sinne von § 2 Abs. 3 IFG NRW." Die gesetzliche Ausnahme soll die Chancengleichheit stärken, die Unabhängigkeit der Prüfenden sicherstellen und die Ausforschung von Prüfungsunterlagen durch Dritte verhindern. Die Zulassung ist der eigentlichen Prüfung hingegen vorgeschaltet und bedarf keines entsprechenden Schutzes.

3.3. Kommunale Tochterunternehmen unterliegen umfassend dem IFG NRW

Gemäß § 2 Abs. 4 IFG NRW gilt eine juristische Person des Privatrechts (etwa eine Gesellschaft mit beschränkter Haftung – GmbH – oder eine Aktiengesellschaft – AG) als auskunftsverpflichtete Behörde, sofern sie öffentlich-rechtliche Aufgaben wahrnimmt. Dies ist – wie das Oberverwaltungsgericht NRW (OVG NRW) bereits im Jahr 2020 entschieden hatte – der Fall, wenn es sich um eine gemeinwohlerhebliche Aufgabe handelt, die im öffentlichen Recht wurzelt, diese Aufgabe durch einen zu ihrer Erfüllung berufenen Hoheitsträger auf ein Privatrechtssubjekt übertragen worden ist und dieses durch den Hoheitsträger beherrscht wird (Urteil vom 17. November 2000, **15 A 4409/18**, siehe dazu auch in diesem Bericht unter 2. Teil 8. und im 26. Bericht unter 2. Teil, Nr. 2.5).

Zu dieser Thematik gibt es inzwischen weitere Entscheidungen. Da die wirtschaftliche Betätigung von Kommunen in der Gemeindeordnung NRW geregelt ist, unterliegen nach einer Entscheidung des Verwaltungsgerichts Düsseldorf kommunale Tochterunternehmen im Bereich der Daseinsvorsorge den Verpflichtungen nach dem IFG NRW (Urteil vom 11. November 2024, **Az. 29 K 8721/22**). Das Urteil betraf einen im Glasfaserausbau tätigen Energieversorger.

In dieselbe Richtung geht auch eine Entscheidung des Verwaltungsgerichts Köln (Urteil vom 9. November 2023, Az. **13 K 4761/18**), welches ein Verkehrsunternehmen als informationspflichtig nach § 2 Abs. 4 IFG NRW einstuft. Diese war bei Redaktionsschluss allerdings noch nicht rechtskräftig, da das beklagte Unternehmen Berufung gegen das erstinstanzliche Urteil eingelegt hat und eine Entscheidung des OVG NRW noch aussteht.

3.4. Föderale Zusammenarbeit ist weitgehend frei von Informationspflichten nach dem IFG NRW

Ein Kläger begehrte erfolglos Zugang zu Berichten der Arbeitsgruppen der Justizministerkonferenz, einem Instrument intraföderaler Zusammenarbeit. Nach einer Entscheidung des OVG NRW (Urteil vom 23. Mai 2023, **Az. 15 A 47/21**) handele es sich bei dieser Koordination der Länderinteressen zwar um Verwaltungstätigkeit im Sinne von § 2 Abs. 1 IFG NRW, so dass der Anwendungsbereich des IFG NRW eröffnet sei. Gemäß § 6 Satz 1 Buchstabe c IFG NRW sei der Informationszugang aber abzulehnen, soweit durch das Bekanntwerden Angaben und Mitteilungen öffentlicher Stellen des Bundes oder anderer Länder ohne deren Zustimmung offenbart würden. Das OVG NRW hat entschieden, dass hiervon auch Gemeinschaftsarbeiten der Bundesländer umfasst sind. Die in den Arbeitsgruppen verfassten Berichte enthielten mehrheitlich oder einstimmig beschlossene Inhalte und stünden den Bundesländern nur in gemeinschaftlicher Verbundenheit zu, auch wenn die Positionen einzelner Länder nicht identifizierbar seien. Die daraus folgende Beschränkung der Verfügungsbefugnis über die Informationen erfordere im Ergebnis die Zustimmung aller beteiligten Länder nach § 6 Satz 1 Buchstabe c IFG NRW.

3.5. Anbieter*innen von Rechtsdatenbanken haben keinen Anspruch auf Herausgabe von Gerichtsentscheidungen

Das IFG NRW findet nach § 2 Abs. 2 nur auf die Verwaltungstätigkeit der Gerichte, nicht aber auf ihre justizielle Tätigkeit, also Urteile oder Beschlüsse, Anwendung. Das OVG NRW hat dazu entschieden, dass das IFG NRW keinen Anspruch auf Veröffentlichung von gerichtlichen Entscheidungen in einer Rechtsprechungsdatenbank gewährt (Beschluss vom 23. Januar 2023, **Az. 15 E 599/22**). Zum einen ziele die Regelung des § 4 Abs. 1 IFG NRW „nicht auf die Veröffentlichung von Informationen gegenüber einem allgemeinen Personenkreis ab, sondern auf die Übermittlung derselben an einen bestimmten Antragsteller". Zum anderen handele es sich bei der Veröffentlichung um eine Verwaltungsaufgabe. Begehrten Antragstellende aber Zugang zu einer Gerichtsentscheidung, so ziele dieses Begehren nicht auf Informationen zu der als Verwaltungsaufgabe eingestuften Veröffentlichung, sondern auf die Gerichtsentscheidung selbst. Diese sei indes nach Art. 97 Abs. 1 Grundgesetz dem besonders geschützten justiziellen Bereich zuzuordnen und damit dem Anwendungsbereich des IFG NRW entzogen.

Weiter wies das Gericht auf die Möglichkeit hin, nach § 124 Satz 3 Justizgesetz NRW (JustG NRW) in Verbindung mit Nr. 4 der Anlage 2 (Gebührenverzeichnis) zu § 124 JustG NRW in Verbindung mit § 8 Abs. 2

Justizverwaltungskostengesetz vorzugehen. Danach kann Dritten, die nicht am Verfahren beteiligt sind, gegen Zahlung von 12,50 Euro eine anonymisierte Abschrift der Entscheidung zugesendet werden.

In diesem Zusammenhang ist ein Beschluss des Verwaltungsgerichts Aachen erwähnenswert: Das Gericht war noch vor fünf Jahren in einem vergleichbaren Fall von der Anwendbarkeit des IFG NRW ausgegangen (Urteil vom 11. Februar 2020, **8 K 276/16**) und hatte hieraus einen Anspruch auf Übersendung anonymisierter Urteilsabschriften bzw. deren Einstellung in die Entscheidungsdatenbank NRWE abgeleitet. Nun hat es diese Rechtsprechung aufgegeben (Beschluss vom 2. Februar 2023, **Az. 8 K 1080/22**). Dabei stellt das IFG NRW eigentlich nicht auf den Ursprung der Information, sondern allein auf das Vorhandensein im Verwaltungsbereich ab (§ 4 Abs. 1 IFG NRW).

3.6. Berichte, die auf staatsanwaltschaftlichen Ermittlungen beruhen, sind nicht zugänglich

Nach § 2 Abs. 2 IFG NRW kann bei den Staatsanwaltschaften Zugang zu Informationen nur betreffend deren Verwaltungstätigkeit, nicht aber zum Bereich der Strafrechtspflege – also der Ermittlungsarbeit – begehrt werden. Das Verwaltungsgericht Düsseldorf hat entschieden, dass Berichte an das übergeordnete Justizministerium NRW sowie dort verfasste, diesbezügliche Vermerke – hier: zu Cum-Ex-Ermittlungsverfahren – ebenfalls nicht beansprucht werden können (Urteil vom 24. August 2023, **Az. 29 K 329/21**). Dem Ministerium steht gemäß §§ 146, 147 Nr. 2 Gerichtsverfassungsgesetz das Recht zu, Weisungen auch zum Bereich der Strafverfolgung zu erteilen. Es sei insoweit wegen der sachlich-inhaltlichen Mitwirkung als Behörde der Staatsanwaltschaft nach § 2 Abs. 2 IFG NRW zu qualifizieren. Soweit Staatsanwaltschaften über Strafsachen an das Ministerium berichten, werde dieses zur Ausübung des Weisungsrechts befähigt. Die ministerielle Tätigkeit zähle diesbezüglich zur Strafrechtspflege. In der Folge sei insoweit bereits der Anwendungsbereich des IFG NRW nicht eröffnet.

3.7. Ratsmitglieder gehen leer aus

Das Verwaltungsgericht Köln hat einen Anspruch auf Informationszugang abgelehnt, weil er von einem Mann in seiner Eigenschaft als Stadtratsmitglied geltend gemacht wurde (Urteil vom 7. September 2023, **Az. 4 K 3440/22**). § 4 IFG NRW berechtige nur natürliche Personen als Bürger*innen, nicht aber Amtsträger*innen, soweit sie eine staatliche Funktion wahrnehmen. Möchten letztere privat einen Anspruch nach dem IFG NRW geltend machen, sollten sie auf Bezugnahmen auf ihr Amt verzichten. Insbesondere sei es schädlich, das amtliche Briefpapier oder die dienstliche E-Mail-Adresse zu verwenden.

4. Aus der Beratungspraxis



4.1 Landtag beschränkt Auskunftsrecht gegenüber öffentlich-rechtlichen Kreditinstituten

Was hat ein neues Gesetz zur Modernisierung des Sparkassenrechts mit dem Recht auf Informationsfreiheit zu tun? Auf den ersten Blick nichts – auf den zweiten Blick sehr viel. Vergleichsweise versteckt findet sich in dem Gesetz eine Änderung, die es öffentlich-rechtlichen Kreditinstituten erlaubt, Informationen zu verweigern, wenn es um die Verwendung öffentlicher Gelder geht.

Am 18. Dezember 2024 hat der Landtag von NRW ein Gesetz beschlossen, das den öffentlich-rechtlichen Kreditinstituten wie ein vorgezogenes Weihnachtgeschenk vorgekommen sein dürfte. Das Gesetz, das sich in erster Linie mit der Modernisierung des Sparkassenrechts beschäftigt, nimmt eher unbemerkt von der Öffentlichkeit zugleich eine Neuregelung vor, die das IFG NRW betrifft. Galt das IFG NRW bislang umfassend auch für die öffentlich-rechtlichen Kreditinstitute wie Sparkassen und die NRW.BANK, sind sie seither in einem wesentlichen Bereich von dessen Verpflichtungen zur Transparenz ausgenommen – nämlich dann, wenn es um Kund*innendaten und damit zugleich um Fördergelder geht.

„Für öffentlich-rechtliche Kreditinstitute gilt dieses Gesetz nur, soweit nicht Zugang zu kundenbezogenen Daten gewährt werden soll, die dem Kreditinstitut aufgrund, aus Anlass oder im Rahmen der Geschäftsverbindung zum Kunden bekannt geworden sind", heißt es in der Neuregelung. Sie soll nur dann nicht gelten, wenn sich Auskunftsansprüche auf Informationen zu „aggregierten, nicht individualisierbaren Daten" beziehen oder „zu Konten in der Zeit des Nationalsozialismus enteigneter oder verfolgter Personen oder zum späteren Umgang der öffentlich-rechtlichen Kreditinstitute mit diesen Konten".

Begründet hat die Landesregierung die Neuregelung damit, dass „die reale Gefahr" bestehe, dass das „Vertrauen in die öffentlich-rechtlichen Kreditinstitute nachhaltig beschädigt" werde, wenn diese über das Recht auf Informationsfreiheit gezwungen würden, Informationen über kundenbezogene Daten herauszugeben. Außerdem gehe es darum, den „Wettbewerbsnachteil" der öffentlich-rechtlichen gegenüber privaten Kreditinstituten abzumildern, da die privaten Institute nicht dem IFG NRW unterliegen.

Verschiedene Sachverständige hatten sich in einer Anhörung im federführenden Haushalts- und Finanzausschuss allerdings gegen eine solche Ausnahme ausgesprochen. Die Regelung führe zu einem beträchtlichen Transparenzdefizit und sei bereits aufgrund ausreichender Ausnahmetatbestände zum Schutz personenbezogener Daten und von Betriebs- und Geschäftsgeheimnissen schlicht nicht erforderlich. Es sei unklar, ob öffentlich-rechtliche Kreditinstitute in wesentlichem Umfang überhaupt von IFG-Anträgen betroffen sind. Die in der Gesetzesbegründung beschriebene „reale Gefahr" für das Vertrauen in die öffentlich-rechtlichen Kreditinstitute sei „ohne konkrete Belege eine Fiktion ohne Realitätsbezug". Zudem komme das IFG NRW seit 22 Jahren ohne eine solche Klausel aus. Die ins Feld geführte Milderung des Wettbewerbsnachteils gegenüber anderen, nicht dem IFG NRW unterworfenen Kreditinstituten, sei mangels wissenschaftlicher Untersuchung unbelegt. Außerdem nähmen die Sparkassen zwar am Wettbewerb teil, jedoch sei nach dem Sparkassengesetz NRW die Gewinnerzielung nicht der Hauptzweck des Geschäftsbetriebs.

Auch die LDI NRW hat diese Einschätzung geteilt und bedauert dementsprechend die Gesetzesänderung. Zwar ist nachvollziehbar, dass in dem Bereich, in denen die öffentlichen Kreditinstitute in Konkurrenz zu privaten Instituten stehen, zusätzliche Bürokratiehürden abgebaut werden sollten. Es ist aber sehr zweifelhaft, ob das IFG NRW in der Praxis überhaupt Bürokratielasten erzeugt. In der Aufsichtspraxis der LDI NRW fehlen Fälle mit Forderungen nach einem Informationszugang im Bankenbereich nahezu völlig, der sich auf das Alltagsgeschäft der Banken bezieht. Wahrscheinlich kommen sie in der Praxis kaum vor, weil potentiell Interessierte wohl ohnehin vom Bestehen eines umfassenden Bankgeheimnisses über die Kontoinformationen der Bankkund*innen ausgehen.

Hinzu kommt das Problem, dass die IFG-Ausnahme, die sich auf kundenbezogene Daten und Geschäftsverbindungen zum Kunden bezieht, sehr offen formuliert und damit weit gefasst ist. Das lässt vermuten, dass von der Anwendung des IFG NRW ein weitaus größerer Bereich ausgenommen sein dürfte als nur solche Daten, die unter das sog. Bankgeheimnis fallen. Es steht zu befürchten, dass dadurch künftig ein Transparenzdefizit auch bei Informationen entsteht, die der Öffentlichkeit weiterhin zugänglich sein sollten. Darüber hatte die LDI NRW die Landesregierung im Gesetzgebungsverfahren informiert.

So müssen die betroffenen Kreditinstitute nun etwa keine Auskunft mehr geben zur Vergabe von Förderkrediten an Unternehmen und Kommunen und zu deren Beratung. Die Bereichsausnahme umfasst auch diese Kunden der öffentlichen Kreditinstitute. Konkret geht es zum Beispiel um Förderkredite und andere Unterstützungsinstrumente für von Flutschäden betroffene Unternehmen und Kommunen. Außerdem ausgenommen sind Informationen im Bereich der Wirtschaftsförderung zu zinsgünstigen Förderkrediten für Betriebsmittelbedarf und Investitionen. Im Bereich der Infrastrukturförderung geht es zudem um Kredite, die Kommunen für Investitionsmaßnahmen nutzen können.

Alle diese Förderprogramme werden mit öffentlichen Geldern finanziert, weshalb die Öffentlichkeit einen Anspruch auf Kenntnis dieser Informationen haben sollte. Auf diesem Betätigungsfeld stehen die öffentlichen Kreditinstitute auch nicht in Konkurrenz zu privaten Banken. Die Kontrollfunktion des IFG NRW ist damit in einem wichtigen Bereich ausgehebelt. Die LDI NRW spricht sich deshalb dafür aus, mindestens eine gesetzliche Einschränkung der IFG-Ausnahme vorzunehmen. Beispielsweise kann man die Ausnahme auf Kund*innenbeziehungen beschränken, in denen die öffentlichen Banken zu privaten Banken in Konkurrenz stehen. Dies tun sie bei der Vergabe öffentlicher Mittel regelmäßig nicht. So könnte ein politisch interessierendes und wichtiges Betätigungsfeld wieder für den Informationszugang geöffnet werden.

Fazit

Das kurz vor Weihnachten verabschiedete Gesetz führt zu einem erkennbaren Transparenzdefizit in NRW im Bereich der öffentlich-rechtlichen Kreditinstitute, und zwar in Bezug auf Informationen, auf deren Kenntnis die Öffentlichkeit einen Anspruch haben sollte. Gerade mit Blick auf das sensible Thema der Verwendung öffentlicher Gelder sollte eine gesetzliche Anpassung diesen wichtigen Bereich wieder transparent machen.

4.2. Dürfen Behörden die Postanschrift von Bürger*innen verlangen, die Informationen beanspruchen?



Personenbezogenen Daten sind sensibel. Deshalb wird die LDI NRW oft mit der Frage konfrontiert, ob und inwieweit diese Daten von einer Behörde erhoben werden dürfen, die einen Antrag nach dem IFG NRW bearbeitet. Die LDI NRW rät weiterhin, die Erforderlichkeit der Erhebung von Adressen im Einzelfall zu prüfen. Mehr Informationsfreundlichkeit und weniger Bürokratie können auch das Behördenimage stärken.

Wenn Informationsfreiheit und Datenschutz aufeinandertreffen, kann das eine gewisse Sprengkraft entfalten. Das IFG NRW gibt Bürger*innen das Recht auf Zugang zu behördlichen Informationen. Haben die öffentlichen Stellen im Gegenzug das Recht, die Postanschrift sowie weitere personenbezogenen Angaben der Antragsteller*innen bei der Bearbeitung ihrer IFG-Anträge zu erheben?

Ein neues Urteil des Bundesverwaltungsgerichts aus dem vergangenen Jahr zum Informationsrecht gegenüber einer Bundesbehörde bringt Unruhe in dieser Frage. Die langjährige Praxis der LDI NRW ist klar: Aus Gründen des Datenschutzes darf die verantwortliche Stelle die Postanschrift sowie weitere personenbezogenen Angaben bei der Bearbeitung von IFG-Anträgen nur dann erheben, wenn diese Daten zur Aufgabenerfüllung erforderlich sind. Diese Voraussetzung ist bei der Bearbeitung von Anfragen nach dem IFG NRW aber nur in Ausnahmefällen erfüllt (siehe dazu auch im 22. Bericht 2015 der LDI NRW unter 12.3 sowie im 23. Bericht 2017 unter 16.3).

Umso erfreulicher war es, dass das Oberverwaltungsgericht NRW (OVG NRW) dies in einem Urteil aus dem Jahr 2022 ähnlich sah – auch wenn sich dieses ausschließlich auf das IFG des Bundes (IFG-Bund) bezog (Urteil vom 15. Juni 2022, Az. 16 A 857/21). In dem zugrundeliegenden Fall hatte

ein Bundesministerium unmittelbar nach Eingang des IFG-Antrags per E-Mail die Postanschrift des Antragstellers angefordert. Nachdem dieser seine Anschrift mitgeteilt hatte, erhielt er die postalische Antwort, dass zu seiner Anfrage keine Informationen vorlägen. In der Folge wandte sich der Antragsteller an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Dieser erließ, nachdem er das Bundesministerium angehört hatte, eine datenschutzrechtliche Verwarnung. Die Erhebung der Postanschrift sei unberechtigterweise erfolgt, da die Anschrift nicht erforderlich gewesen sei, um dem Antragsteller mitzuteilen, dass die beantragte Information gar nicht vorhanden sei.

Gegen diese Verwarnung erhob das Bundesministerium Klage. In der zweiten Instanz kam das OVG NRW zu dem Schluss, dass die Kenntnis der konkreten Identität sowie der Postanschrift in diesem Fall nicht notwendig war, um den IFG-Antrag zu bearbeiten.

Das Bundesverwaltungsgericht hat dieses Urteil nun aber 2024 wieder kassiert (Urteil vom 20. März 2024, **Az. 6 C 8.22**). Es hat entschieden, dass es zur Bearbeitung eines Antrags nach dem Bundes-IFG regelmäßig erforderlich sei, den Namen und eine zustellungsfähige Postadresse der antragstellenden Person zu kennen Das Bundes-IFG enthalte zwar keine ausdrückliche Rechtsgrundlage zur Erhebung dieser Daten, so das Bundesverwaltungsgericht. Im zugrundeliegenden Fall sei die Datenerhebung jedoch aus zwei Gründen erforderlich gewesen: zur ordnungsgemäßen Bearbeitung des Antrags sowie zur Bekanntgabe der abschließenden Entscheidung. Um sicher zu gehen, dass hinter dem Antrag tatsächlich eine natürliche Person – und nicht etwa ein Bot – stehe, seien der Klarname und die Adresse erforderlich. Außerdem könne nur dann zuverlässig geprüft werden, ob der Antrag wegen bereits vorhandener Kenntnis der Information abgelehnt werden kann. Schließlich sei die Identität für Maßnahmen zur Vollstreckung der Gebühren und Auslagen und die Stellungnahme Dritter erforderlich.

Zwar hat die Entscheidung für NRW keine unmittelbare Bedeutung, da sie sich ausschließlich auf das IFG-Bund bezieht. Die Auffassung des Bundesverwaltungsgerichts könnte aber auf Gerichte in NRW ausstrahlen. Nicht auszuschließen ist, dass auch Fälle aus NRW einmal beim Bundesverwaltungsgericht landen.

Die LDI NRW empfiehlt öffentlichen Stellen dennoch, Namen und Postanschrift nicht vorschnell und reflexartig immer dann zu erheben, wenn ein IFG-Antrag gestellt wird. Es ist im Einzelfall zu prüfen, ob und inwieweit diese Daten zur Aufgabenerfüllung tatsächlich erforderlich sind. Dies kann etwa der Fall sein, wenn davon auszugehen ist, dass der Informationszugang gebührenpflichtig sein wird. Die Befürchtung von eingesetzten Chatbots, die die Behörde lahmlegen könnten, kann auch ein Grund sein, aber dafür sollte es konkrete Anhaltspunkte geben.

Insbesondere bei einfachen, kostenfreien Anfragen ohne Drittbeteiligung und in Fällen, in denen die Information ohnehin an jede und jeden herausgegeben werden müsste oder dürfte, sollten Informationszugangsanträge hingegen weiterhin beantwortet werden, ohne Adresse oder Identität abzufragen. Stellt die Behörde nach Prüfung des IFG-Antrags fest, dass sie beabsichtigt, den Antrag abzulehnen, ist es ratsam, dies der oder dem Antragstellenden per E-Mail mitzuteilen und nachzufragen, ob ein rechtsmittelfähiger Bescheid gewünscht wird. Vor diese Wahl gestellt, hat dann die oder der Antragstellende selbst die Möglichkeit, Identität und Adresse mitzuteilen, um einen förmlichen Bescheid zu erhalten, oder darauf zu verzichten und so anonym zu bleiben.

Fazit

Personenbezogene Daten der Antragstellenden dürfen nur erhoben werden, wenn dies zur Aufgabenerfüllung erforderlich ist. In der Anwendungspraxis hat sich eine unbürokratische Bearbeitung ohne zusätzliche Datenerhebungen bewährt und spart der Verwaltung auch zusätzliche Arbeit.

4.3. Öffentliche Gutachten sind für die Bürger*innen nicht tabu



Staatliche Stellen verweigern gern den Einblick in Gutachten, die sie in Auftrag gegeben haben – insbesondere bei nicht erwünschten Ergebnissen. Meist wird pauschal darauf verwiesen, dass der Entscheidungsbildungsprozess geschützt werden müsse. Dabei haben Bürger*innen einen Anspruch darauf zu wissen, was in den Gutachten steht. Nur ist dieser Anspruch nicht so einfach durchzusetzen.

Ob Denkmalschutz, Gebäudesanierung oder Stadtentwicklung: die öffentliche Verwaltung setzt bei ihrer Arbeit auch auf Begutachtung durch bezahlte Expert*innen, um am Ende die richtige Entscheidung zu treffen. Doch nicht jeder*jede Bürger*in ist mit dem Ergebnis einverstanden, immer wieder kommt es vor, dass öffentliche Entscheidungen hinterfragt werden und dazu Einblick in die Gutachten verlangt wird. Doch gibt es einen Anspruch auf Einsichtnahme? Die LDI NRW hat sich mehrmals mit derartigen Fällen beschäftigen müssen, weil die öffentlichen Stellen mauerten. Zu Unrecht, wie zwei Fälle zeigen.

Im ersten Fall hatte der Antragsteller bei seiner Stadt Einsicht in eine Machbarkeitsstudie verlangt. Sie war in Auftrag gegeben worden, um einen Überblick über mögliche zukünftige Nutzungsmöglichkeiten einer denkmalgeschützten Mühle zu erhalten. Die Stadt verweigerte allerdings den Zugang zu der Studie unter Hinweis auf § 7 Abs. 2 Buchstabe a) IFG NRW. Danach ist der Antrag auf Informationszugang abzulehnen, sofern sich der Inhalt der Information auf den behördlichen Willensbildungsprozess bezieht. Konkret begründete die Stadt ihre Ablehnung damit, dass die Machbarkeitsstudie den Willensbildungsprozess der Stadt zum Umgang mit dem Gebäude abbilde.

Diese Argumentation ist aus Sicht der LDI NRW jedoch nicht tragfähig. Gutachten bilden regelmäßig nur die Grundlage für den Willensbildungsprozess, sind aber nicht dessen Bestandteil. Dies wäre aber die Voraussetzung dafür, dass der Verweigerungsgrund des § 7 Abs. 2 Buchstabe a) IFG NRW greift. Bereits 2006 hat das Oberverwaltungsgericht NRW entschieden, dass zwischen den Grundlagen und Ergebnissen der Willensbildung auf der einen Seite und dem eigentlichen Prozess der Willensbildung auf der anderen Seite zu unterscheiden ist (Urteil vom 9. November 2006, Az. 8 A 1679/04). Der Verweigerungsgrund des § 7 Abs. 2 Buchstabe a) IFG NRW greift nur für Anordnungen, Äußerungen und Hinweise, die die Willensbildung steuern sollen. Geschützt sind damit allein Unterlagen, die den Prozess der Willensbildung inhaltlich unmittelbar wiedergeben, nicht aber die dem Willensbildungsprozess zugrunde liegenden Sachinformationen.

So lag der Fall auch bei der Machbarkeitsstudie. Die LDI NRW hat die Stadt deshalb aufgefordert, dem Bürger das Gutachten zugänglich zu machen. Da die Stadt dieser Aufforderung nicht folgte, hat die LDI NRW die Verweigerung zusätzlich beanstandet. Der Antragsteller bekam trotzdem keine Einsicht in das Gutachten. Die Möglichkeiten der LDI NRW zur Unterstützung einer antragstellenden Person waren damit erschöpft.

Im zweiten Fall hatte ein Bürger das Gutachten zum Zustand der Hauptfeuerwehrwache einsehen wollen. Das wurde zuerst mit dem Hinweis abgelehnt, das Gutachten befinde sich noch in Arbeit bzw. in Abstimmung. Erst als die LDI NRW die Stadt zur Stellungnahme aufforderte, erteilte diese einen Ablehnungsbescheid. Darin führte sie – ähnlich wie

im ersten Fall – aus, dass die Unterlage zunächst nur dazu diene, den Entscheidungsprozess der Behördenleitung zu unterstützen und die Entscheidung vorzubereiten, sich daher auf den Prozess der Willensbildung beziehe. Eine Entscheidung der Behördenleitung sei zudem bislang nicht getroffen. Eine Bekanntgabe der Unterlagen würde zu diesem Zeitpunkt die Effektivität des Verwaltungshandelns in nicht unerheblicher Weise beeinträchtigen. Die LDI NRW hat dazu klargestellt, dass die Standortbeschreibung nebst Empfehlungen und Vorschlägen des beauftragten Büros zu einer möglichen Entwicklung des Standorts der Feuerwache als solche kein Willensbildungsprozess der Behörde sei. Der Antragsteller erhob schließlich Klage vor dem Verwaltungsgericht, bekam Recht und so den gewünschten Zugang zu dem Gutachten. Die Stadt hatte durch das Klageverfahren einen erheblichen Mehraufwand.

Fazit

Egal wie sie genannt werden: Machbarkeitsstudie, Standortbeschreibung, Auswertung oder Studie – letztlich sind es immer Gutachten, die aus öffentlichen Mitteln finanziert werden. Sie müssen in der Regel zugänglich gemacht werden, denn sie bilden lediglich eine Grundlage der Willensbildung und sind in den seltensten Fällen Teil des Meinungsbildungsprozesses der Behörde selbst. Solche Unterlagen, die mit öffentlichen Mitteln bezahlt werden, sollen grundsätzlich auch der Öffentlichkeit zur Verfügung stehen.

4.4. Nicht jeder Vertrag ist vom Informationszugang ausgenommen

Öffentliche Stellen können nicht davon ausgehen, dass sie ihre Vertragsangelegenheiten generell geheim halten dürfen, weil es sich um Betriebs- und Geschäftsgeheimnisse handelt. Das muss vielmehr in jedem Einzelfall sorgfältig geprüft werden.

Muss eine Behörde oder eine Stadt alle Informationen, die sie besitzt, der Öffentlichkeit zugänglich machen? Das IFG NRW kennt durchaus Ausnahmen. Gerade dann, wenn es sich um Betriebs- und Geschäftsgeheimnisse etwa von Kommunen handelt, können Informationen dazu dem Zugriff für jedermann entzogen sein. Doch ganz so einfach ist das nicht. Die Schwierigkeit liegt wie so oft im Detail, wie ein Fall zeigt, der die LDI NRW 2024 beschäftigt hat – und den Kommunen wie Bürger*innen kennen sollten.

Ein Einwohner hatte seine Stadt gebeten, ihm Akteneinsicht in Fernwärmeverträge zwischen der Stadt und einem Energieversorger zu gewähren. In der Sache ging es um einen Anschluss- und Benutzungszwang an eine zentrale Fernwärmeversorgung für Teile eines Bebauungsplangebietes, der in der Satzung der Stadt festgeschrieben ist. Die Bewohner dieses Gebietes wurden damit verpflichtet, ihre Wärme von dem betreffenden Energieversorger zu beziehen. Der Antragsteller machte geltend, dass ca. 1.000 Bürger*innen von dieser Regelung betroffen seien. Ihn interessierte, ob ein erheblicher Einfluss der Kommune im Vertrag geregelt ist, der einen Anschlusszwang mit einer privaten Betreiberfirma rechtfertigen könnte. Zudem wollte er klären, ob der Betreibervertrag Optionen für eine Umrüstung des Heizkraftwerks auf umweltfreundliche Energieträger vorsieht.

Die Stadt jedoch lehnte den Antrag auf Informationszugang unter dem pauschalen Hinweis auf eine Vorschrift im IFG NRW ab, wonach Betriebs- und Geschäftsgeheimnisse von einem Informationszugang ausgeschlossen sind (§ 8 IFG NRW). Sie verwies darauf, dass sich der Energieversorger unter Berufung auf diese Ausnahme gegen eine Veröffentlichung ausgesprochen habe. Der Bürger wandte sich daraufhin an die LDI NRW – mit Erfolg.

Generell gilt: Derartige Ablehnungen des Informationszugangs sind zunächst einmal ausreichend zu begründen. Ein bloßer Hinweis etwa auf § 8 IFG NRW genügt nicht. Die informationssuchende Person muss nachvollziehen können, warum der Zugang nicht gewährt wird.

Konkret setzt die Ablehnung mittels § 8 IFG NRW weiteres voraus. So müsste durch die Übermittlung der Information ein Betriebs- oder Geschäftsgeheimnis offenbart werden und dadurch ein wirtschaftlicher Schaden entstehen. Als Betriebs- oder Geschäftsgeheimnisse werden allgemein alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig sind, sondern nur einem begrenzten Personenkreis zugänglich und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat.

Ein solches Interesse liegt vor, wenn die Offenlegung der Information den eigenen Wettbewerb schwächen oder den fremden Wettbewerb stärken kann. Maßgeblich ist, inwieweit mögliche Mitbewerber*innen tatsächlich einen wirtschaftlichen Nutzen aus der Offenlegung der begehrten Informationen ziehen können. Hinzukommen muss schließlich ein durch die Offenlegung entstehender wirtschaftlicher Schaden. Ein solcher ist anzunehmen, wenn davon auszugehen ist, dass sich die Wettbewerbssituation durch die Offenbarung des Betriebs- oder Geschäftsgeheimnisses nachhaltig verschlechtern wird.

Gerade diese Voraussetzung, einen entstehenden Schaden belegen zu müssen, kann aber der Knackpunkt in solchen Verfahren sein. Im kon-

kreten Fall nämlich konnte die Stadt nicht darlegen, welcher Schaden ihr durch die Offenlegung der Fernwärmeverträge entstehen würde. Zunächst hielt die Stadt nach Rücksprache mit ihrem Vertragspartner auch gegenüber der LDI NRW daran fest, dass § 8 IFG NRW als Ausschlusstatbestand greife und die gewünschten Informationen nicht zur Verfügung gestellt werden müssten. Die Ablehnung enthielt im Wesentlichen aber nur die Wiedergabe der Stellungnahme des Energieversorgers, der seinerseits lediglich den Gesetzestext des § 8 IFG NRW zitierte.

Das aber reicht nicht. Auskunftspflichtige Stelle ist nicht der Vertragspartner einer Kommune, sondern die öffentliche Stelle selbst. Eine eigenständige Prüfung hatte die Stadt aber gar nicht vorgenommen. Bis zum Schluss konnte sie außerdem nicht erläutern, worin sie einen möglichen Schaden sieht. Nach mehreren Monaten gab sie schließlich die zuvor verwehrten Informationen zu den Fernwärmeverträgen an den Antragsteller heraus.

Fazit

Bürger*innen können durchaus einen Anspruch auf Zugang zu Verträgen haben, die von einer öffentlichen Stelle geschlossen wurden. Nicht jedes Betriebs- und Geschäftsgeheimnis muss geheim bleiben. Das hat seinen Grund auch darin, dass das IFG NRW unter anderem dem Zweck dient, die Verwendung von Steuermitteln offen zu legen und den Bürger*innen damit eine gewisse Kontrolle staatlichen Handelns zu ermöglichen.

4.5. Auch Unternehmen können auskunftspflichtig sein

Das IFG NRW verpflichtet öffentliche Stellen, den Bürger*innen gegenüber transparent mit Informationen umzugehen. Aber gilt das Auskunftsrecht der Bürger*innen auch gegenüber juristischen Personen des Privatrechts, etwa GmbHs oder Aktiengesellschaften, die unter hoheitlicher Verwaltung stehen? Die Erfahrung der LDI NRW zeigt: Das Gesetz gilt für mehr Stellen als gedacht.

Immer wieder kommt es vor, dass Verbraucher*innen Auskunft auch von Einrichtungen verlangen, die nicht öffentlich-rechtlich organisiert sind, sondern privatrechtlich. Ob Energieversorgung oder Müllentsorgung - Städte übertragen ihre Aufgaben nicht selten auf Unternehmen in Form von GmbHs oder Aktiengesellschaften. Das aber führt häufig

zu Irritationen. Müssen sich auch juristische Personen des Privatrechts unter bestimmten Voraussetzungen der Transparenzpflicht des IFG NRW beugen?

Auch 2023 und 2024 hat sich die LDI NRW mit dieser Frage beschäftigt. Die Antwort ist vom Einzelfall abhängig und wird auch von der aktuellen Rechtsprechung mitbestimmt. Ganz anschaulich macht das ein Fall, in dem die LDI NRW um Vermittlung gebeten wurde. Der Antragsteller hatte sich mit einem IFG-Antrag an eine GmbH gewandt und um Informationen zu deren Arbeit gebeten. Die GmbH entwickelt ein Umsetzungskonzept für den regionalen Transformationsprozess im rheinischen Braunkohlerevier – besser bekannt als „Förderung des Strukturwandels".

Bei der Prüfung durch die LDI NRW spielt insbesondere § 2 Abs. 4 des IFG NRW eine Rolle. Dort wird eine Behördenfiktion für bestimmte Aktivitäten festgelegt. Sie lautet: „Sofern eine natürliche oder juristische Person des Privatrechts öffentlich-rechtliche Aufgaben wahrnimmt, gilt sie als Behörde im Sinne dieses Gesetzes." Hiermit soll sichergestellt werden, dass sich die Verwaltung durch eine Auslagerung ihrer Aufgaben auf Private nicht ihrer Informationspflicht entziehen kann.

Wie die Vorschrift genau zu verstehen ist, hat bereits 2020 das Oberverwaltungsgericht NRW klar definiert (Urteil vom 17. November 2020, 15 A 4409/18; siehe dazu auch 26. Bericht unter 2. Teil, Nr. 2.5). Danach nimmt eine Privatrechtsperson eine öffentlich-rechtliche Aufgabe wahr, „wenn es sich um eine gemeinwohl-erhebliche Aufgabe handelt, die im öffentlichen Recht wurzelt, diese Aufgabe durch einen zu ihrer Erfüllung berufenen Hoheitsträger auf das Privatrechtssubjekt übertragen worden ist und dieses durch den Hoheitsträger beherrscht wird." Die vom Oberverwaltungsgericht NRW konkretisierten Voraussetzungen treffen damit oft auch auf Stellen zu, die man nicht auf Anhieb als potentiell Auskunftsverpflichtete nach dem IFG NRW im Blick hatte. Hierzu gehört nach einer Entscheidung des Verwaltungsgerichts Düsseldorf etwa auch ein kommunales Energieversorgungsunternehmen in seiner Eigenschaft als Telekommunikationsdienstleistungsunternehmen (Urteil vom 11. November 2024, **Az. 29 K 8721/22**).

Dementsprechend kam die LDI NRW nach Prüfung des Falles der Gesellschaft zur Förderung des Strukturwandels zu dem Ergebnis, dass die GmbH als auskunftspflichtige Stelle im Sinne des IFG NRW anzusehen ist. Und zwar, weil

- ihre Aufgabe gemeinwohlerheblich ist, da die Förderung des Strukturwandels laut eigener Homepage des Unternehmens einen positiven Effekt auf die Menschen in der Region haben soll sowie auf die dortige Wirtschaft, Arbeitsplätze, Lebensqualität und den Klimaschutz,

- diese Aufgabe im öffentlichen Recht wurzelt und auf die GmbH übertragen worden ist, indem die GmbH im Strukturstärkungsgesetz Kohleregionen vom 8. August 2020 ausdrücklich als zuständig für den Strukturwandel im Rheinischen Revier genannt wird und

- schließlich auch eine hoheitliche Beherrschung gegeben ist, da laut Handelsregister ihre Gesellschafter mehrheitlich Kommunen, die Industrie- und Handelskammer sowie die Handwerkskammer sind.

Das Unternehmen hat dennoch an seiner abweichenden Auffassung festgehalten. Der Antragsteller hat deshalb den Klageweg beschritten. Wie das Verwaltungsgericht Aachen entscheiden wird, bleibt abzuwarten. Die Klage ist aktuell dort anhängig.

Fazit

Die Verwaltung darf sich durch eine Auslagerung ihrer Aufgaben auf Private nicht ihrer Informationspflicht nach dem IFG NRW entziehen. Das hat auch die Rechtsprechung der vergangenen Jahre bestätigt. Sie stärkt damit das Recht auf Informationsfreiheit.

4.6. Gebührenberechnung bei Informationsanträgen: Gute Kommunikation verhindert den Rechtsstreit



Die Erhebung von Gebühren durch Behörden führt immer wieder zu Schwierigkeiten. Einerseits werden Gebührenforderungen nicht immer nachvollziehbar begründet, andererseits ist den Antragsteller*innen vielfach nicht bewusst, welchen Aufwand ihr Antrag auf Informationszugang für die Behörde bedeutet.

Nicht jede Tätigkeit einer Behörde ist kostenlos. Ob es um einen neuen Reisepass geht oder ein Führungszeugnis – der entstehende Aufwand muss häufig bezahlt werden. Das gilt auch für Anträge auf Zugang zu bestimmten Informationen nach dem IFG NRW. Eine öffentliche Stelle ist danach berechtigt, für die Bereitstellung von Informationen, die mit einem umfangreichen Verwaltungsaufwand verbunden ist, Gebühren zu erheben (§ 11 IFG NRW in Verbindung mit der zugehörigen Verwaltungsgebührenordnung).

Allerdings ist die Festlegung der Höhe der Gebühren oft nicht einfach – und das Wissen der Bürger*innen dazu vielfach begrenzt. Deshalb führen Gebührenerhebungen immer wieder auch zu Missverständnissen zwischen Behörde und Antragsteller*innen.

Auch 2024 musste die LDI NRW hier vermitteln. Ein Antragsteller hatte um Übersendung einer Übersicht aller Gutachter*innenaufträge gebeten, die in einem bestimmten Zeitraum durch die zuständige Behörde erteilt worden waren. Der Informationszugang wurde in Aussicht gestellt, jedoch verbunden mit der Ankündigung, eine Gebühr in Höhe von 300 Euro zu erheben. Da der Antragsteller dies nicht nachvollziehen konnte und die Forderung für zu hoch befand, wandte er sich an die LDI NRW.

Bei der Gebührenfestsetzung sind einige Kriterien zu beachten.

- Der Bescheid muss konkrete und schlüssige Ausführungen zum Gebührenrahmen und zur Gebührenhöhe enthalten: Weshalb etwa handelt es sich um einen umfangreichen Verwaltungsaufwand? Wie wurde die Gebühr konkret berechnet? Welcher Aufwand ist wofür in welcher Zeit entstanden? Welche einzelnen Arbeitsschritte waren erforderlich?

- Bei der Höhe einer Gebühr ist auch das sog. Äquivalenzprinzip zu beachten. Danach muss ein angemessenes Verhältnis zwischen der Gebühr und dem Wert der von der auskunftspflichtigen Stelle erbrachten Leistung bestehen. Für die Ermittlung der Höhe der festzusetzenden Gebühren darf der Verwaltungsaufwand nicht der alleinige Maßstab sein.

Im vorliegenden Fall ließ das Schreiben an den Antragsteller tatsächlich nicht hinreichend erkennen, wie der Gebührenbetrag konkret ermittelt wurde. Die LDI NRW trat deshalb an die Behörde heran und bat darum, dem Antragsteller eine ausführliche und nachvollziehbare Begründung der Gebührenhöhe unter den beschriebenen Gesichtspunkten zu geben. Es folgte eine detaillierte Stellungnahme, die im Ergebnis belegte, dass die angekündigte Gebührenhöhe in einem durchaus adäquaten Verhältnis zum Aufwand stand. Die Behörde bat den Antragsteller zudem um Mitteilung, ob er seinen Antrag auf Informationszugang unter dieser Voraussetzung aufrechterhalten oder ggf. einschränken wolle.

Der Mann schränkte daraufhin seinen Ausgangsantrag ein – und erhielt am Ende sogar einen kostenfreien Informationszugang.

Fazit

Wenn eine Behörde nach erster kursorischer Prüfung feststellt, dass es sich um keine „einfache" und somit kostenfreie Auskunft handelt, sollte sie den Antragsteller*innen nicht nur eine möglichst realistische Abschätzung der Höhe der Gebühren mitteilen, sondern auch eine nachvollziehbare Begründung für den entstehenden Aufwand. Antragsteller*innen erhalten so die Chance, sich ein möglichst genaues Bild von den drohenden Kosten zu machen, und können dann entscheiden, ob sie den Antrag eingrenzen möchten.

4.7. Tödlicher Unfall – Behörden müssen schnell informieren

Gerade bei gravierenden Ereignissen wie einem tödlich verlaufenden Verkehrsunfall haben Bürger*innen ein Interesse daran zu wissen, welche Maßnahmen ergriffen wurden, um solche Unfälle künftig zu verhindern. Und sie haben auch ein Recht darauf, dies zügig zu erfahren.

Verkehrsunfälle passieren leider immer wieder. Und manchmal enden sie besonders tragisch. Bürger*innen wollen dann häufig auch wissen, was von den zuständigen Behörden getan wird, um solche Ereignisse künftig zu verhindern. Bleibt eine Antwort aus, kommt mitunter die LDI NRW ins Spiel.

So auch in einem Fall, der exemplarisch veranschaulicht, dass ein Recht auf schnelle Transparenz existiert und wie dieses umzusetzen ist. In der Gemeinde des betroffenen Bürgers hatte sich auf einer unübersichtlichen Kreuzung ein tödlicher Fahrradunfall ereignet. Der Mann wollte daraufhin von der Stadt wissen, welche verkehrstechnischen Maßnahmen sie in Reaktion auf den Radunfall ergriffen hatte.

Die Stadt aber reagierte nicht. Auf seinen Antrag nach dem IFG NRW und weitere Schreiben erhielt er keinerlei Antwort. Er wandte sich daraufhin an die LDI NRW mit der Bitte einzugreifen. Doch auch das Auskunftsersuchen der LDI NRW, obwohl zuständig für die Überprüfung von Transparenzanliegen, sowie mehrere Erinnerungen blieben inhaltlich unbeantwortet.

Erst nach einer durch die LDI NRW ausgesprochenen Beanstandung erhielt der Antragsteller schließlich eine Zusammenfassung der Maßnahmen. So hatte die Stadt eine Roteinfärbung der betroffenen Radfurt beschlossen, also der Führung des Radverkehrs über die Kreuzung. Außerdem sollten zusätzlich Absperrmaßnahmen errichtet werden, um den Radverkehr besser in den Furtbereich zu lenken.

Die Absperrung war allerdings zum Zeitpunkt der Antwort noch nicht umgesetzt. Als Begründung für die verzögerte Antwort gab die Stadt an, dass die individuelle Prüfung „ein wenig Zeit" erfordert habe. Tatsächlich musste der Antragsteller im Ergebnis fast ein Jahr warten, bis ihm die geforderten Informationen mitgeteilt wurden.

Für die LDI NRW ist dies Anlass, noch einmal alle öffentlichen Stellen daran zu erinnern, dass IFG-Anträge regelmäßig binnen eines Monats beantwortet werden sollen. So heißt es im IFG NRW: „Die Information soll unverzüglich, spätestens innerhalb eines Monats nach Antragstellung, zugänglich gemacht werden." Dies gilt insbesondere dann, wenn die Antwort so einfach ist wie in dem konkreten Fall. Wichtig ist, dass

Kommunen sich vergegenwärtigen, dass sie im Ansehen bei den Bürger*innen gewinnen, wenn sie Antworten fristgerecht geben. Transparent und zeitnah zu informieren, ist ein gutes Marketing für die eigene Arbeit.

Fazit

Das IFG NRW kann Bürger*innen helfen, zügig Klarheit darüber zu erhalten, welche Schutzmaßnahmen eine Kommune nach einem Verkehrsunfall trifft. Für die Kommune ist eine schnelle Unterrichtung bestes Marketing.

4.8. Wer Informationen von einer schwierigen Behörde will, kann es auch mit „Plan B" versuchen

Das kann vorkommen: Eine Behörde verfügt über viele Stellungnahmen anderer öffentlicher Stellen, verweigert aber unzulässigerweise die Herausgabe dieser Informationen. Das IFG NRW enthält für dieses Problem manchmal noch eine „Plan-B-Lösung".

In städtebaulichen Verfahren agiert meist nicht eine Behörde allein. Vielmehr sind verschiedene Träger öffentlicher Belange eingebunden. Dies sind Stellen, die nach dem Baugesetzbuch (BauGB) im Vorfeld einer Bauleitplanung zu beteiligen sind, damit öffentliche Belange bei der Baumaßnahme umfassend berücksichtigt werden können. Je nach Einzelfall werden zum Beispiel andere Behörden mit ins Boot geholt oder benachbarte Gemeinden, aber auch privatrechtlich organisierte Institutionen. Und sie alle geben meist Stellungnahmen zu dem Bauvorhaben ab.

Für Bürger*innen, die all diese Stellungnahmen einsehen möchten, erschwert das die Situation, insbesondere, wenn sie auf eine im Umgang schwierige Behörde treffen. Doch die Lage ist nicht hoffnungslos – wie ein Fall zeigt, in dem die LDI NRW um Vermittlung gebeten wurde.

In dem Fall ging es um ein Bauleitplanverfahren, an dem die Stadt insgesamt elf verschiedene Stellen im Vorfeld beteiligt hatte. Der Antrag

des Antragstellers auf Zugang zu sämtlichen Stellungnahmen wurde abgelehnt. Die Stadt begründete dies zum einen mit den nach ihrer Ansicht spezielleren Regelungen im BauGB, welche eine Anwendung des IFG NRW ausschließen würden. Zum anderen gehörten die Stellungnahmen nach Auffassung der Stadt zum behördlichen Willensbildungsprozess – der von Ansprüchen nach dem IFG NRW ausgenommen ist.

Auch die Intervention der LDI NRW führte zunächst nicht zum Erfolg. Die Stadt verhielt sich rechtswidrig, da in dem konkreten Fall die von der Stadt vorgebrachten Ablehnungsgründe nicht gelten. Weder hebeln die Regeln im BauGB das IFG NRW aus, da die im BauGB vorgesehene Beteiligung der Öffentlichkeit gerade nicht die Stellungnahmen der Träger öffentlicher Belange mit umfasst. Noch sind die Stellungnahmen unmittelbarer Bestandteil des Willensbildungsprozesses der Behörde, sondern nur dessen Grundlage. Auch dieser Ausschlussgrund galt damit nicht. Die Stadt hielt jedoch an ihrer Auffassung fest.

Da die LDI NRW Behörden nicht zur Herausgabe von Unterlagen verpflichten kann, wäre allenfalls eine Beanstandung in Frage gekommen, die aber die Stadt mit ihrem festgefahrenen Standpunkt voraussichtlich auch nicht zum Einlenken gebracht hätte.

Dennoch konnte dem Antragsteller am Ende geholfen werden, und zwar über einen „Plan B", der mühseliger ist, aber hier effektiv war. So blieb dem Antragsteller ein aufwendiges Klageverfahren erspart. Dem Mann wurde empfohlen, zunächst bei der Stadt in Erfahrung zu bringen, welche Träger öffentlicher Belange in dem betreffenden Verfahren beteiligt waren. Dann sollte er sich einzeln an jede beteiligte Stelle wenden und dort jeweils beantragen, Zugang zu den gegenüber der Stadt abgegebenen Stellungnahmen zu bekommen. Da in diesem Fall die Träger öffentlicher Belange weitgehend auskunftspflichtig nach dem IFG NRW waren, konnte er so letztlich alle Stellungnahmen einsammeln. Er erhielt sogar die Unterlagen einer Stelle, die nicht dem Anwendungsbereich des IFG NRW unterfiel. Besonders ärgerlich: Die unnötige Weigerung der Kommune führte dazu, dass anstatt nur einer Stelle insgesamt gleich zwölf öffentliche Stellen mit der Bearbeitung des IFG-Begehrens beschäftigt waren, was den Verwaltungsaufwand für alle Seiten grundlos erhöhte.

Fazit

Wenn die LDI NRW informationspflichtige Stellen nicht überzeugen kann, empfiehlt sie auch schon mal einen „Plan B", um den Informationssuchenden ein Klageverfahren zu ersparen.

4.9. Behörden sollten klar kommunizieren, wenn ihnen begehrte Informationen nicht vorliegen

Bürger*innen dürfen darauf vertrauen, dass öffentliche Stellen ehrlich mit ihnen umgehen. Dieses Vertrauen ist gefährdet, wenn eine auskunftspflichtige Stelle einen Antrag auf Informationszugang aufwendig ablehnt – und sich später herausstellt, dass sie die beantragte Information gar nicht besitzt.

Es ist eigentlich ganz einfach. Bürger*innen in NRW haben nach dem IFG NRW nur dann einen Anspruch auf behördliche Informationen, wenn diese auch tatsächlich vorhanden sind. Dazu gehören laut Gesetz „alle in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder auf sonstigen Informationsträgern vorhandenen Informationen, die im dienstlichen Zusammenhang erlangt wurden". Informationsträger sind dabei alle Medien, „die Informationen in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder in sonstiger Form speichern können".

Dennoch kommt es vor, dass sich öffentliche Stellen mit dieser Regelung schwertun. So auch in einem Fall, mit dem sich die LDI NRW im vergangenen Jahr zu beschäftigen hatte. Ein Bürger hatte von der Stadt Zugang zu internen Handlungsanweisungen verlangt. Die Stadt jedoch lehnte den Antrag ab und führte dazu diverse Gründe an. So seien die Handlungsanweisungen organisatorische Maßnahmen – und solche Maßnahmen seien durch das DSG NRW vom Recht auf Informationsfreiheit ausgenommen. Außerdem beziehe sich die verlangte Information auf den Bereich des behördlichen Willensbildungsprozesses. Auch in diesem Fall dürften Behörden nach dem IFG NRW Anträge auf Informationszugang ablehnen.

Nach Einschalten der LDI NRW stellte sich allerdings heraus, dass die erbetenen Handlungsanweisungen bei der Stadt gar nicht vorhanden waren. Sie waren nur mündlich erteilt worden und daher keine auf einem Informationsträger gespeicherte Information im Sinne des IFG NRW. Die zuvor bemühten Ablehnungsgründe spielten deshalb gar keine Rolle.

Festzuhalten bleibt, dass eine solche Vorgehensweise nicht im Sinne einer guten und eindeutigen Kommunikation zwischen Behörde und Bürger*in ist. Sofern beantragte Informationen nicht vorhanden sind, empfiehlt es sich, dies dem Antragstellenden gegenüber von vornherein klarzustellen. Anderer Ablehnungsgründe bedarf es dann nicht.

Es verwirrt vielmehr, wenn Ablehnungsgründe ausgeführt werden, die am Ende gar nicht zum Tragen kommen. Der Antragstellende wird unter Umständen dann sogar bezweifeln, dass die Informationen nicht vorhanden

sind, weil er glaubt, dass die weiteren Ablehnungsgründe ansonsten nicht vorgetragen worden wären. Dies kann im schlimmsten Fall zu einer Eskalation führen. Behörden handeln folglich auch im eigenen Interesse, wenn sie von Anfang an offen agieren.

Fazit

Wenn die begehrten Informationen nicht vorhanden sind, sollten Behörden dies klar kommunizieren und keine weiteren Ablehnungsgründe bemühen. Das ist auch im Interesse der Verwaltung, um für die Bürger*innen glaubhaft und authentisch zu bleiben.

Anhang zum Datenschutzbericht

Veröffentlichungen der Datenschutzkonferenz 2024

1. Entschließungen der Datenschutzkonferenz 2024

19.12.2024 – Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen![1]

Die Gesetzgeber und Regierungen der EU, des Bundes und der Länder streben einen digitalen Wandel an, in dessen Mittelpunkt der Mensch steht (siehe z. B. Europäische Erklärung zu den digitalen Rechten und Grundsätzen in der digitalen Dekade; 2023/C 23/1). Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) erkennt das Potential, das der digitale Wandel in allen Lebensbereichen für Wirtschaft und Gesellschaft birgt. Sie unterstützt deswegen das Leitbild einer menschenzentrierten Digitalisierung als ein wichtiges politisches Ziel in der Europäischen Union. Seine Umsetzung und Verwirklichung durch unterschiedliche Akteure muss das Grundrecht auf informationelle Selbstbestimmung im Blick behalten und insbesondere die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten beachten. Speziell in der Daseinsvorsorge sieht die Datenschutzkonferenz daher die Notwendigkeit, diesen menschenzentrierten Ansatz zum Schutz derjenigen, die nicht digital agieren können oder wollen, gesetzlich zu flankieren.

Seien es zentrale Verkehrsdienstleistungen, die Energie- oder Wasserversorgung oder öffentlich geförderte kulturelle Dienstleistungen, der Trend zur Digitalisierung hält überall Einzug. Wenn für die Inanspruchnahme solcher Dienstleistungen die Nutzung elektronischer Kommunikationswege (z. B. Internet), die Eröffnung eines digitalen Kontos oder die Nutzung einer Smartphone-App vorausgesetzt werden, kann das dazu führen, dass bestimmte Menschen von der Inanspruchnahme solcher Daseinsvorsorgeleistungen ausgeschlossen werden. Das betrifft all diejenigen, die aufgrund körperlicher oder geistiger Beeinträchtigung, ihres Alters (Minderjährige ebenso wie Ältere), Technikferne oder fehlender Mittel nicht in der Lage sind, die digitale Technik zu nutzen, oder die in Ausübung ihres Grundrechts auf informationelle Selbstbestimmung ihre Daten nicht preisgeben wollen. Dieser Trend ist auch eine Herausforderung für die Grundrechte auf Datenschutz und Achtung des Privatlebens aus Art. 8 und Art. 7 der Charta der Grundrechte

---

1 Der Bayerische Landesbeauftragte für den Datenschutz und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit haben die Entschließung abgelehnt.

der Europäischen Union (GRCh) sowie auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) in ihrem jeweiligen Anwendungsbereich.

Vor diesem Hintergrund weist die Datenschutzkonferenz darauf hin, dass bei der Leistungserbringung gemäß Art. 6 Abs. 1 Buchst. b DSGVO nur die Verarbeitung der für einen Vertrag erforderlichen personenbezogenen Daten zulässig ist. Die Erforderlichkeit der Datenverarbeitung bezieht sich auf den Hauptgegenstand des Vertrags – sie muss also für die Inanspruchnahme der Leistung der Daseinsvorsorge unerlässlich sein. Außerdem ist der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO zu berücksichtigen, wobei die Verarbeitung auf den für den Zweck erforderlichen Umfang zu begrenzen ist. Bei einer auf Einwilligung basierenden Datenverarbeitung ist deren Freiwilligkeit und mithin die Rechtmäßigkeit der Verarbeitung in Frage zu stellen, wenn die betroffenen Personen einer sozialen oder ökonomischen Drucksituation ausgesetzt sind, die ihnen eine „echte oder freie Wahl" (vgl. Erwägungsgrund 42 Satz 5 DSGVO) unmöglich machen.

Vor diesem Hintergrund macht die Datenschutzkonferenz auch auf die besondere Bedeutung der Prinzipien von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Data Protection by Design and Default) nach Art. 25 DSGVO aufmerksam. Der Verantwortliche hat bereits bei der Planung von Digitalisierungsprojekten, aber auch bei ihrer Realisierung insbesondere geeignete Maßnahmen zur Datenminimierung zu treffen. Die Datenschutzkonferenz unterstreicht, dass solche Maßnahmen nachhaltig zur Vertrauenswürdigkeit digitaler Angebote beitragen können. Zugleich sind die in Art. 25 DSGVO verbindlich ausgestalteten Prinzipien kein optionales Angebot der Verantwortlichen, sondern die notwendige Voraussetzung für ein datenschutzkonformes digitales Angebot der Daseinsvorsorge.

Allein mit Mitteln des Datenschutzes sind allerdings befriedigende Lösungen für die Menschen, die wegen fehlender digitaler Möglichkeiten von wichtigen Leistungen der Daseinsvorsorge ausgeschlossen sind, nicht erreichbar. Zum einen kann die rechtliche Durchsetzung des Datenschutzes in möglichen gerichtlichen Auseinandersetzungen viel Zeit in Anspruch nehmen, in denen Betroffene keine schnelle Teilhabe erhalten. Zum anderen sind auch nicht alle gesellschaftspolitischen Aspekte einer menschenzentrierten Digitalisierung an Datenschutzregelungen gebunden. Es bedarf hier vielmehr klarer gesetzlicher Leitplanken, um die menschenzentrierte Digitalisierung voranzubringen. Die Notwendigkeit solcher Maßnahmen aus Verbraucherschutzsicht hat jüngst die 20. Verbraucherschutzministerkonferenz vom 14. Juni 2024 unterstrichen (vgl. Beschluss Nr. 25 + 27: Sicherstellung einer nichtdigitalen Kundenkommunikation und analogen Teilhabe am wirtschaftlichen Leben).

Die Datenschutzkonferenz appelliert an die Gesetzgeber von Bund und Ländern, flankierende gesetzliche Maßnahmen im Bereich der Daseinsvorsorge zu prüfen, die die Rahmenbedingungen einer fairen Teilhabe derjenigen regeln, die keinen digitalen Zugang zu unverzichtbaren Dienstleistungen der Daseinsvorsorge haben oder nicht haben wollen.

20.09.2024 – Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden

Bereits jetzt setzen einige Behörden automatisierte biometrische Gesichtserkennungssysteme im öffentlichen Raum ein und berufen sich dabei auf unspezifische strafprozessuale Normen.[2] Hierbei werden nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) der einschlägige Rechtsrahmen und die Freiheitsrechte der Betroffenen – also potentiell aller Bürgerinnen und Bürger – nicht hinreichend beachtet. Die bestehenden Regelungen in der Strafprozessordnung bieten für biometrische Gesichtserkennung im öffentlichen Raum keine Grundlage. Aktuell gibt es zudem Bestrebungen der Politik, das Instrument der automatisierten biometrischen Gesichtserkennung in unterschiedlichen rechtlichen Zusammenhängen zu erlauben.

Eine Regelung durch den Gesetzgeber wäre hierbei nur in einem engen Rahmen mit den europäischen und nationalen Grundrechten der betroffenen Personen vereinbar.

Der Einsatz von Gesichtserkennungssystemen kann ein sehr intensiver Eingriff in die Grundrechte der betroffenen Personen sein. Die Intensität hängt insbesondere von der Art der ausgewerteten Daten, der eingesetzten Technik und dem Grad der Automatisierung ab. Von besonderer Bedeutung ist die Streubreite der Maßnahme, wie z. B. beim Einsatz von Gesichtserkennungssystemen im öffentlichen Raum. Erfasst die Analyse viele Menschen und zudem solche, die dafür keinerlei Anlass gegeben haben, führt dies zu einem noch intensiveren Eingriff. Relevant sind ferner eine eventuelle Heimlichkeit der Maßnahme und das erhebliche Risiko von Fehlerkennungen. Diese können auch für unschuldige Menschen zu intensiven Folgeeingriffen, wie z. B. Freiheitsentziehungen, führen.

---

2 So wurde etwa im Frühjahr 2024 bekannt, dass eine sächsische Polizeidirektion über ein Gesichtserkennungs-system verfügt, welches bereits für Ermittlungsverfahren in verschiedenen Bundesländern genutzt wurde. Als Rechtsgrundlagen wurden §§ 100h, 163f StPO für die Aufzeichnung von Bildern auf öffentlichen Straßen und § 98a StPO für den Abgleich mittels automatisierter Gesichtserkennung herangezogen.

Aus diesem Grund hat der europäische Gesetzgeber in der KI-Verordnung[3] bestimmte Anwendungen ausgeschlossen und für andere Anwendungen enge Grenzen bestimmt.

Sofern nach der KI-Verordnung und dem Verfassungsrecht Regelungsspielraum für den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als zwingend erforderlich betrachtet, muss er spezifische, verhältnismäßige Rechtsgrundlagen für den Einsatz von Gesichtserkennungssystemen schaffen. Hierin sind in Abhängigkeit von der Eingriffsintensität hinreichende Eingriffsschwellen, ausreichende Anforderungen an den Rechtsgüterschutz und zusätzliche Schutzmechanismen festzulegen.

Zu dieser Thematik hat der Europäische Datenschutzausschuss (EDSA) Leitlinien erlassen. Auch nach Ansicht des EDSA darf Gesichtserkennungstechnologie nur unter strikter Einhaltung des einschlägigen Rechtsrahmens und ausschließlich in solchen Fällen verwendet werden, in denen die Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit belegbar erfüllt sind.

Sofern und soweit der Gesetzgeber den entsprechenden Einsatz nach sorgfältiger Prüfung als unbedingt erforderlich betrachtet, fordert die DSK, sich mit den rechtlichen Vorgaben intensiv auseinanderzusetzen und diese zu beachten.

11.09.2024 – Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern

In seinem Urteil vom 26. Oktober 2023 (Az. C-307/22) hat sich der Europäische Gerichtshof (EuGH) zum Verhältnis des Rechts auf Einsicht in die Patientenakte aus § 630g BGB und des Rechts auf Kopie personenbezogener Daten aus Art. 15 Abs. 3 DS-GVO geäußert.

Das Gericht stellte fest, dass der Patient oder die Patientin einen Anspruch auf eine unentgeltliche erste Kopie seiner oder ihrer Akte hat. Durch

---

3 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

eine nationale Regelung wie § 630g Abs. 2 S. 2 BGB darf dem Patienten oder der Patientin keine Kostenlast hierfür auferlegt werden. Der Verantwortliche kann jedoch für alle weiteren Kopien ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen.

Zwar kann nach den Ausführungen des EuGHs eine nationale Regelung, die vor dem Inkrafttreten der DS-GVO erlassen wurde, in den Anwendungsbereich des Art. 23 Abs. 1 Buchst. i DS-GVO fallen und damit den Umfang der u. a. in Art. 15 DS-GVO vorgesehenen Pflichten und Rechte einschränken. Eine solche Möglichkeit erlaubt es jedoch nicht, eine nationale Regelung zu erlassen bzw. eine bestehende Regelung anzuwenden, die der betroffenen Person zum Schutz der wirtschaftlichen Interessen des Verantwortlichen die Kosten für eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung durch den Verantwortlichen sind, auferlegt.

Im Übrigen stellte der EuGH fest, dass der Antrag des Patienten oder der Patientin nicht zu begründen ist. Nach Ausführungen des EuGHs kommt es nicht auf die Motivation des Antragstellers oder der Antragstellerin auf den Erhalt der Kopie an.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGHs nicht nur dringender Handlungsbedarf für den Bundesgesetzgeber besteht, § 630g Abs. 2 S. 2 BGB den Vorgaben der DS-GVO anzupassen. Auch die Berufsordnungen der Heilberufskammern enthalten regelmäßig entsprechende Regelungen zur Kostenerstattung für die Herausgabe von Kopien aus der Patientenakte (vgl. § 10 Abs. 2 a. E. Muster-Berufsordnung der Bundesärztekammer; § 12 Abs. 4 Muster-Berufsordnung der Bundeszahnärztekammer; § 11 Abs. 1 Muster-Berufsordnung der Bundespsychotherapeutenkammer), die den Vorgaben der DS-GVO und der Rechtsprechung des EuGHs widersprechen.

Während der Bundesgesetzgeber eine Änderung des BGB noch in dieser Legislaturperiode vornehmen wird, ist offen, ob und ggf. wann es auch zu den notwendigen berufsrechtlichen Anpassungen kommen wird. Im Sinne eines möglichst einheitlichen Rechtsrahmens und aus Gründen der Rechtsklarheit fordern die deutschen Aufsichtsbehörden daher die Heilberufskammern auf, die berufsrechtlichen Regelungen zeitnah an die Vorgaben aus der DS-GVO anzupassen. Die bestehenden zivil- und berufsrechtlichen Regelungen, die für die Bereitstellung einer Erstkopie eine Kostenpflicht für den Patienten oder die Patientin vorsehen, sind nicht anwendbar. Bis eine Änderung der jeweiligen Berufsordnung erfolgt ist, sind die Kammermitglieder über die Entscheidung des EuGHs zum Anspruch des Patienten bzw. der Patientin auf eine kostenlose Kopie der Patientenakte zu informieren und zu einem rechtskonformen Vorgehen anzuhalten.

15.05.2024 – Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert sowohl alle relevanten Stakeholder – insbesondere Leitungen, Träger und Interessenvertretungen der Krankenhäuser – als auch die verantwortlichen Akteure in Politik und Verwaltung sowie die Gesetzgeber des Bundes und der Länder dazu auf, sich frühzeitig mit den datenschutzrechtlich relevanten Auswirkungen der für die Zukunft zu befürchtenden weiteren Krankenhausschließungen zu befassen.

In den vergangenen Monaten hat die Zahl an Schließungen und Insolvenzen von Krankenhäusern bundesweit stark zugenommen. Die DSK nimmt dies insbesondere im Hinblick auf die in den Einrichtungen vorgehaltenen besonders schutzbedürftigen Behandlungsdokumentationen der Patientinnen und Patienten mit Sorge zur Kenntnis. Wiederholt wurden die Datenschutzaufsichtsbehörden mit Fällen konfrontiert, in denen eine sichere Aufbewahrung und der Zugang der Betroffenen zu den Patientendaten nicht gewährleistet waren. Teilweise bestand sogar die Gefahr, dass sich Unbefugte Zugang zu den Krankenakten verschaffen konnten.

Die DSK weist in diesem Zusammenhang auf Folgendes hin:
Datenschutzrelevante Herausforderungen für Klinikbetreiber und Insolvenzverwalter im Zusammenhang mit Krankenhausschließungen

Die Erfahrungen der Aufsichtsbehörden zeigen, dass mangels Insolvenzmasse die Kosten zur weiteren Aufbewahrung der Patientenakten häufig ab einem gewissen Zeitpunkt nicht mehr durch den Insolvenzverwalter getragen werden können. Hat die Suche nach anderen rechtlich Verantwortlichen keinen Erfolg, gibt es im Bereich der Krankenhausbehandlung keine bundes- oder landesgesetzlichen Festlegungen, durch wen und in welcher Form die weitere Aufbewahrung einschließlich der Löschung der Patientendaten erfolgen muss und in welcher Weise die Patientinnen und Patienten Zugang zu den sie betreffenden Behandlungsdokumentationen erhalten. Insbesondere fehlen hier vergleichbare Regelungen, wie sie sich vereinzelt in Heilberufsgesetzen der Länder finden, in denen unter bestimmten Voraussetzungen eine Notverantwortung der Heilberufskammern bei der Schließung ambulanter Arztpraxen festgelegt wurde (z. B. § 22 Abs. 2 des rheinland-pfälzischen Heilberufsgesetzes, § 4 Abs. 1 Satz 4 ff. HBKG BW, § 7 Abs. 3 SächsHKaG).

Aus Sicht der DSK hat dieser Zustand starke nachteilige Auswirkungen auf den datenschutzrechtlich gebotenen Schutz der Gesundheitsdaten und die effektive Wahrnehmung der Betroffenenrechte der Patientinnen und Patienten:

Patientenakten enthalten Gesundheitsdaten im Sinne von Artikel 4 Nr. 15 der DS-GVO, die eine besondere Kategorie personenbezogener Daten nach Artikel 9 DS-GVO dar stellen. Aufgrund ihrer Sensibilität muss ihnen ein besonderer Schutz zukommen. Dies ist derzeit im Falle der Insolvenz von Krankenhausträgern oder ungeplanter Schließungen von einzelnen Einrichtungen nur unzureichend rechtlich geregelt.

Nur sofern ein Insolvenzverfahren läuft, können Patientinnen und Patienten regelmäßig über den Insolvenzverwalter Einsicht in ihre Akte erlangen. Sobald das Insolvenzverfahren jedoch beendet ist oder mangels Masse nicht eröffnet wird, ist aufgrund fehlender Regelungen offen, durch wen und unter welchen technisch organisatorischen Anforderungen Krankenhausakten aufzubewahren, datenschutzkonform zu löschen und wie Patientenrechte zu gewährleisten sind. Dies ist sowohl aus datenschutzrechtlicher Sicht als auch im Interesse einer im Einzelfall gebotenen medizinischen Weiterbehandlung nicht hinzunehmen. Es bedarf deshalb zeitnaher effektiver Lösungen, die den weiteren Umgang sowohl mit papiergebundenen als auch mit elektronisch geführten Patientenakten im Falle von Klinikschließungen datenschutzkonform festlegen. Denn die datenschutzrechtlichen Vorgaben, wie sie beim fortlaufenden Krankenhausbetrieb zu beachten sind, gelten auch nach einer Betriebseinstellung fort.

Denkbare Lösungsansätze aus datenschutzrechtlicher Sicht

Die DSK hält unter anderem folgende Bausteine für geeignet, um eine datenschutzkonforme Lösung der aufgezeigten Problematik zu finden:

- In Anlehnung an bereits bestehende Regelungen in den Landeskrankenhausgesetzen von Nordrhein-Westfalen (§ 34c Abs. 1 KHGG NRW) und Hessen (§ 12 Abs. 5 HKHG) sollten die Krankenhäuser bundesweit dazu verpflichtet werden, entsprechende Konzepte zur weiteren Verwahrung der Patientenakten für den Fall der Insolvenz oder der ungeplanten Schließung anzufertigen. Diese sollten der zuständigen Fachaufsicht vorgelegt werden.

- Aufgrund der aufgezeigten Probleme im Kontext von Insolvenzen regt die DSK an, dass sich die Länder mit einer Finanzierungs-Lösung befassen, damit in dringenden Fällen Aufbewahrungen und Sicherungen von Patientenakten für einen Übergangszeitraum weiter finanziert werden können. So sieht z. B. das Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen in § 34c Abs. 2-6 KHGG NRW die Einrichtung von Patientenaktensicherungsfonds vor.

- Solange keine geeigneten landesrechtlichen Regelungen existieren, sollten die relevanten Stakeholder, insbesondere Leitungen,

Träger und Interessenvertretungen der Krankenhäuser, gemeinsam datenschutzkonforme Lösungen entwickeln, um im Bedarfsfall die kurzfristige sichere Aufbewahrung von Patientenakten geschlossener Kliniken sicherzustellen. Dabei könnten auch Vertreter der Datenschutzaufsicht beratend beteiligt werden.

- Die DSK regt an, dass sich die Gesundheitsministerkonferenz bei ihrer nächsten Zusammenkunft mit der Thematik befasst und Lösungsmöglichkeiten erarbeitet. Dabei sollte eine lückenlose Regelung der Notverantwortung für Patientendaten geschlossener Krankenhäuser angestrebt werden – etwa wie dies in den Heilberufsgesetzen oder Pflegekammergesetzen einzelner Länder durch die Zuständigkeit der Kammern geschehen ist.

Die DSK appelliert nachdrücklich an die Entscheidungsträger, bestehende Regelungslücken zu schließen und im Interesse der betroffenen Patientinnen und Patienten für Rechtsklarheit und Rechtssicherheit zu sorgen.

2. Beschlüsse der Datenschutzkonferenz 2024

11.09.2024 – Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals

Die Veräußerung eines Unternehmens kann grundsätzlich auf zwei Wegen erfolgen, nämlich entweder durch Übertragung von Anteilen an einer Gesellschaft als „Share Deal" oder durch Übertragung von Vermögenswerten und/oder Wirtschaftsgütern als „Asset Deal". Während die Verarbeitung von personenbezogenen Daten im Rahmen eines „Share Deals", abgesehen von Prüfungshandlungen während einer Due Diligence Prüfung, unproblematisch möglich ist, da nur die Anteile an einer Gesellschaft übertragen werden, diese ansonsten unverändert fortgeführt wird und mangels Änderung in der Person der oder des Verantwortlichen grds. keine Übermittlung personenbezogener Daten erfolgt, bedarf es bei der Übermittlung von personenbezogenen Daten im Rahmen eines „Asset Deals" in datenschutzrechtlicher Hinsicht einer differenzierten Betrachtung, die im Folgenden dargestellt wird.

Unter dem Begriff des Asset Deals ist dabei ein Unternehmenskauf zu verstehen, bei dem Wirtschaftsgüter/Vermögenswerte (engl.: Assets) eines Unternehmens wie beispielsweise Grundstücke, Gebäude, Maschinen, Kundenstamm, Rechte etc., im Rahmen der Singularsukzession auf die Erwerberin oder den Erwerber übertragen werden. Ein Asset Deal liegt zum Beispiel vor, wenn eine Einzelunternehmerin oder ein Einzelunternehmer (Veräußerer)[4] ihren bzw. seinen Betrieb an eine Nachfolgerin oder einen Nachfolger (Erwerber) übergibt und dabei beispielsweise die Maschinen, den Kundenstamm, die Firmierung etc. übernimmt und den Betrieb fortführt.

Insbesondere Einzelkaufleute, Handwerkerinnen und Handwerker oder Personengesellschaften sind bei einem Betriebsübergang mit zusätzlichen datenschutzrechtlichen Herausforderungen konfrontiert, die sich bei dem – allein Kapitalgesellschaften möglichen – Share Deal gar nicht stellen. Die nachfolgenden Hinweise sollen den Betriebsinhaberinnen und -inhabern helfen, diesen Anforderungen gerecht zu werden.

4 Die Begriffe Veräußerer und Erwerber, Gläubiger und Schuldner, Zedent und Zessionar werden im Folgenden ausschließlich rechtstechnisch verwendet und weisen nicht auf das Geschlecht der Personen hin, die tatsächlich an dem Rechtsgeschäft beteiligt sind.

I. Übermittlung personenbezogener Daten vor Abschluss des Asset Deals, sog. Due Diligence

Zum Zeitpunkt der Vertragsverhandlungen zwischen Veräußerern und potentiellen Erwerbern – also vor Abschluss eines Vertrages (des Asset Deals) – ist die Übermittlung von personenbezogenen Daten grundsätzlich unzulässig. Das bezieht sich insbesondere auf Daten von Kundinnen und Kunden, Lieferantinnen und Lieferanten und von Beschäftigten. Die Übermittlung dieser Daten an den potenziellen Erwerber ist aber zulässig aufgrund einer im Einzelfall vorliegenden freiwillig erteilten Einwilligung der von der Übermittlung betroffenen Personen. Im Rahmen der fortgeschrittenen Übernahmeverhandlungen kann im Einzelfall ein berechtigtes Interesse die Übermittlung von Daten besonders hervorgehobener Personen aus den vorgenannten Gruppen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO rechtfertigen. Bspw. kann es sich dabei um Hauptvertragspartnerinnen und -partner, Personal mit Führungsverantwortung und / oder für das Geschäft zentralen Kompetenzen handeln.

Im Beschäftigungsverhältnis ist bei der Beurteilung der Freiwilligkeit die Abhängigkeit der Beschäftigten zu berücksichtigen. Freiwilligkeit kann ausnahmsweise vorliegen, wenn von Veräußerern und ihren Beschäftigten gleichgerichtete Interessen verfolgt werden. Die Einwilligung hat hier in aller Regel schriftlich oder elektronisch zu erfolgen, siehe § 26 Abs. 2 BDSG.

II. Daten von Kundinnen und Kunden

Bei der Übermittlung von Daten der Kundinnen und Kunden vom Veräußerer an den Erwerber im Rahmen eines Asset Deals ist zwischen den Stadien einer Vertragsanbahnung, einer laufenden vertraglichen Beziehung des Veräußerers mit der jeweiligen Kundin oder dem jeweiligen Kunden und einer vollständig erfüllten oder beendeten vertraglichen Beziehung zwischen Veräußerer und der Kundin oder dem Kunden zu unterscheiden.

1. Vertragsanbahnung

Eine Vertragsanbahnung liegt vor, wenn zwischen dem Veräußerer und der Kundin oder dem Kunden konkrete Vertragsverhandlungen geführt werden. Führt die Kundin oder der Kunde die Verhandlungen mit dem Erwerber von sich aus rügelos fort, so ist die Verarbeitung der für die Fortsetzung erforderlichen personenbezogenen Daten gerechtfertigt durch Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Im Übrigen ist eine Übermittlung nur dann zulässig, wenn eine Überprüfung durch den Veräußerer ergibt, dass den eigenen berechtigten Interessen an der Übermittlung keine überwiegenden Interessen der Kundin oder des Kunden entgegenstehen (Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO). Den berechtigten Interessen der Kundin oder des Kunden kann in aller Regel durch eine Widerspruchslösung Rechnung getragen werden. Den Kundinnen und Kunden wird dazu die Datenübermittlung an den Erwerber mit einer angemessenen Frist (etwa 6 Wochen) für einen möglichen Widerspruch angekündigt.

2. Laufende vertragliche Beziehungen
Eine laufende vertragliche Beziehung zwischen Veräußerer und der Kundin oder dem Kunden im hier gemeinten Sinne liegt vor, wenn der Veräußerer Verpflichtungen gegenüber einer Kundin oder einem Kunden aus einem Vertragsverhältnis (beispielweise Erbringung einer Leistung, Herstellung eines Werkes, Übergabe einer Kaufsache, Zahlung des Kaufpreises, Zahlung des Dienst- oder Werklohnes, Erfüllung etwaiger Mängelgewährleistungspflichten) hat, die noch nicht erloschen sind (beispielsweise durch Erfüllung) bzw. deren gesetzliche Verjährungs- oder vertragliche Garantiefristen noch nicht abgelaufen sind. Hierbei ist insbesondere darauf zu achten, dass beispielsweise Mängelgewährleistungsansprüche regelmäßig erst nach mehreren Jahren verjähren, so dass bis zu diesem Zeitpunkt von einer laufenden vertraglichen Beziehung auszugehen ist. Der Veräußerer sollte daher im Vorfeld des Abschlusses des „Asset Deals" sorgfältig prüfen, zu welchen Kundinnen und Kunden noch eine laufende vertragliche Beziehung besteht und zu welchen nicht.

Werden die laufenden Verträge zwischen dem Veräußerer und den jeweiligen Kundinnen und Kunden mit der zivilrechtlich erforderlichen Genehmigung letzterer auf den Erwerber übertragen, so dass dieser die Verträge übernimmt und selbst neuer Schuldner und Gläubiger der jeweiligen Kunden wird (Vertragsübernahme), so erfüllt der Erwerber den Vertrag mit dem Kunden. Damit kann der Erwerber die für die durch ihn vorzunehmende Vertragserfüllung erforderliche Verarbeitung der Daten des Kunden auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO stützen. Entsprechendes gilt für den Fall der bloßen Schuldübernahme nach § 415 Abs. 1 BGB.

Soll allerdings der Erwerber lediglich den Veräußerer von dessen Schuld gegenüber den jeweiligen Kundinnen und Kunden freistellen, handelt es sich hierbei um eine bloße Erfüllungsübernahme. Wird eine Erfüllungsübernahme zwischen Erwerber und Veräußerer vereinbart, ist zu prüfen, ob einer Übertragung der Daten der Kundinnen und Kunden vom Veräußerer auf den Erwerber überwiegende Interessen der Kundin oder des Kunden i. S. v. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO entgegenstehen. Dies dürfte regelmäßig hinsichtlich der für die Erfüllung erforderlichen Daten nicht der Fall sein, weil die Kundin oder der Kunde vor allem an der Erfüllung interessiert sein dürfte und diese in der Regel durch den Erwerber besser gewährleistet werden kann, als durch den Veräußerer. Überwiegen allerdings im Einzelfall die Interessen an der Nichtübertragung der Daten, ist eine wirksame Einwilligung der betroffenen Kundin oder des Kunden erforderlich.

3. Beendete vertragliche Beziehung
Sofern der Veräußerer beabsichtigt, Daten ehemaliger Kundinnen und Kunden ohne laufende Verträge (Altdaten) dem Erwerber zur Erfüllung der gesetzlichen Aufbewahrungsfristen zu übermitteln, ist der Abschluss eines Vertrages über eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO

erforderlich. Diese Daten dürfen zwar übermittelt werden, aber eben nur zum Zwecke gesetzlicher Aufbewahrungsfristen genutzt werden. Der Erwerber hat diese Daten zwingend von den Daten der Kundinnen und Kunden mit einer laufenden vertraglichen Beziehung zu trennen („Zwei-Schrank-Lösung").

Denkbare Alternative ist, dass entsprechende Daten der Kundinnen und Kunden beim Veräußerer verbleiben. Dieser kann die Daten als Verantwortlicher entweder selbst bis zum Ablauf der gesetzlichen Aufbewahrungsfristen speichern oder ein Dienstleistungsunternehmen im Wege einer Auftragsverarbeitung damit beauftragen.

Der Erwerber darf die zur Erfüllung der Aufbewahrungsfristen übergebenen Daten nur dann zu eigenen Zwecken nutzen, wenn hierfür eine wirksame Einwilligung der Kundinnen und Kunden jeweils vorliegt. (Die Daten können dann aus dem „Aufbewahrungsschrank" in den „Schrank für aktive Kundinnen- und Kundenbetreuung" übernommen werden.)

4. Werbung durch den Erwerber

Soweit Kontaktdaten der Kundinnen und Kunden nach den unter 2.1 und 2.2 genannten Kriterien vom Erwerber verarbeitet werden durften, können diese regelmäßig gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in dem Umfang für Werbezwecke genutzt werden, wie dies auch durch den Veräußerer zulässig gewesen wäre. Dies ist dann nicht der Fall, wenn überwiegende Interessen der Kundin oder des Kunden entgegenstehen. Insbesondere bei Werbemaßnahmen mithilfe elektronischer Post oder Telefon ist § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu beachten. Danach erfordert insbesondere die Werbung per Telefon oder per E-Mail grundsätzlich eine vorherige ausdrückliche Einwilligung. Soweit es sich bei der kontaktierten Person nicht um eine Verbraucherin oder einen Verbraucher handelt, reicht im Falle von Werbung mittels eines Telefonanrufes eine mutmaßliche Einwilligung aus. Die Ausnahme des § 7 Abs. 3 UWG (elektronische Werbung ohne Einwilligung) findet regelmäßig keine Anwendung, da nach § 7 Abs. 3 Nr. 1 UWG derjenige, der die elektronische Postadresse verwendet, diese im Rahmen eines Vertragsabschlusses direkt bei der Kundin oder dem Kunden erhoben haben muss. Bei einem vorvertraglichen Schuldverhältnis besteht noch kein Vertragsverhältnis. Soweit eine bestehende Schuld gem. § 415 BGB durch den Erwerber übernommen wird, erhält dieser die E-Mail-Adresse in der Regel vom Veräußerer und nicht von der Kundin oder vom Kunden selbst.

Im Übrigen wird auf die Orientierungshilfe der DSK zur „Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DS-GVO" verwiesen.2

5. Besondere Kategorien nach Art. 9 Abs. 1 DS-GVO der Daten von Kundinnen und Kunden

Besondere Kategorien von Daten der Kundinnen und Kunden, wie beispielsweise Gesundheitsdaten, können nur im Wege der informierten und ausdrücklichen Einwilligung nach Art. 9 Abs. 2 Buchst. a, Art. 7 DS-GVO vom Veräußerer auf den Erwerber übermittelt werden.

6. Bankdaten

Die Bankverbindungen (IBAN) können in den Fallgruppen der Ziffern 2.1 (Vertragsanbahnung) und 2.2 (laufende vertragliche Beziehungen) – soweit die tatbestandlichen Voraussetzungen vorliegen – über Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO an den Erwerber mit übermittelt werden, im Übrigen aber nur nach ausdrücklicher Einwilligung der Kundin oder des Kunden. Soweit vom Erwerber kein vom Veräußerer übergeleiteter Vertrag abzuwickeln ist, kann er kein berechtigtes Interesse an den Daten zur Bankverbindung geltend machen. Unabhängig von der Übermittlung der Bankverbindungsdaten benötigt der Erwerber neue Einzugsermächtigungen der Inhaberinnen und Inhaber der Kontoverbindung, wenn er einen Bankeinzug von Forderungen beabsichtigt.

7. Daten von Kundinnen und Kunden im Falle offener Forderungen

Die Übertragung offener Forderungen richtet sich zivilrechtlich nach den §§ 398 ff BGB (Forderungsabtretung). In diesem Zusammenhang stehende Daten darf der Zedent (Alt-Gläubiger/Alt-Unternehmen) an den Zessionar (Neu-Gläubiger/Neu-Unternehmen) – gestützt auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO – übermitteln. Überwiegende Gegeninteressen bestehen dann, wenn die Abtretung durch Vereinbarung ausgeschlossen ist (§ 399 2. Alt. BGB). In diesen Fällen bleibt allerdings die Möglichkeit, den Erwerber oder einen Dritten zur Einziehung der Forderung im fremden Namen zu ermächtigen. Auch hier dürfen die zum Einzug erforderlichen personenbezogenen Daten gem. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO übermittelt werden.

III. Personenbezogene Daten von Lieferantinnen oder Lieferanten und deren Beschäftigten

Soweit keine schutzwürdigen Gegeninteressen erkennbar sind, können aktuelle und für den Erwerber relevante personenbezogene Daten von Lieferantinnen und Lieferanten oder deren Beschäftigten nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO vom Veräußerer auf den Erwerber übermittelt werden. Insbesondere bei geschäftlichen Kontaktdaten dürften der Übermittlung regelmäßig keine überwiegenden Interessen entgegenstehen. Die Lieferantinnen oder Lieferanten dürften in der Regel sogar ein Interesse daran haben, dass eine bestehende Geschäftsbeziehung mit einem neuen Erwerber fortgesetzt wird.

IV. Beschäftigtendaten

Die Übermittlung von Beschäftigtendaten zur Vertragsdurchführung im Rahmen von „Asset-Deals" vom Veräußerer auf den Erwerber kann – wenn es sich um einen Betriebs- oder Betriebsteilübergang nach § 613a BGB handelt – zum Zeitpunkt des Betriebs- oder Betriebsteilübergangs regelmäßig jedenfalls auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO[5] und, soweit besondere Kategorien von personenbezogenen Daten betroffen sind, auf § 26 Abs. 3 BDSG[6] gestützt werden. Der Veräußerer verarbeitet die Beschäftigtendaten dabei zur Erfüllung des Vertrages mit der oder dem Beschäftigten und zwar für die Beendigung beziehungsweise Abwicklung des Beschäftigungsverhältnisses zwischen ihm sowie den betroffenen Beschäftigten.

Der Erwerber darf die Beschäftigtendaten spiegelbildlich zur Erfüllung des Arbeitsvertrages nach § 613a BGB in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO und Art. 9 Abs. 2 Buchst. b DS-GVO in Verbindung mit § 26 Abs. 3 BDSG verarbeiten.

Allerdings kann es auch besondere Fallkonstellationen geben, in denen eine Datenübermittlung durch den Veräußerer auf den Erwerber nicht oder nicht vollständig erlaubt sein wird, unter anderem:

- Vertragsverhandlungen

  Zum Zeitpunkt von bloßen Vertragsverhandlungen zwischen Veräußerern und potentiellen Erwerbern – also vor Abschluss eines Vertrages über den Übergang eines Betriebs und/oder Betriebsteils gemäß § 613a BGB – ist die Übermittlung von Beschäftigtendaten grundsätzlich unzulässig. Eine Übermittlung wird im Einzelfall möglicherweise nur mit einer wirksamen[7] Einwilligung der Beschäftigten zulässig sein.[8]

---

5 Es bestehen – etwa aus Sicht des BAG, vgl. Az. 1 ABR 14/22, Beschluss vom 09.05.2023, Tz. 64 – Zweifel an der Europarechtskonformität und damit Anwendbarkeit des § 26 Abs. 1 Satz 1 BDSG im Zusammenhang mit einen Betriebs- oder Betriebsteilübergang nach § 613a BGB; vgl. EuGH, Rs. C-34/21, vom 30.03.2023 sowie BAG, a. a. O., Tz. 64. Über Art. 288 AEUV gilt die DS-GVO als Verordnung der EU – und damit zumindest Art. 6 Abs. 1 Buchst. b DS-GVO – als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zur Erfüllung (unter anderem) eines Arbeitsvertrages unmittelbar in allen Mitgliedstaaten.

6 Gegen § 26 Abs. 3 BDSG bestehen keine unionsrechtlichen Bedenken; vgl. BAG, a. a. O., Tz. 48 ff.

7 Es müssen die gesetzlich geregelten Voraussetzungen für eine freiwillige und damit rechtswirksame Einwilligung beachtet werden, § 26 Abs. 2, Abs. 3 Satz 2 BDSG. Weitere Hinweise hierzu finden Sie in dem Kurzpapier Nummer 20 der DSK zur „Einwilligung nach der DS-GVO" unter dsk_kpnr_20.pdf (datenschutzkonferenz-online.de).

8 Datenverarbeitungen im Rahmen einer „Due Diligence-Prüfung" werden vorliegend nicht behandelt, vgl. hierzu Ausführungen auf Seite 1 dieses Dokuments

- **Information der Beschäftigten durch Erwerber vor dem Betriebs-/Betriebsteilübergang**

  Beschäftigte, die von einem Betriebs- oder Betriebsteilübergang nach § 613a BGB betroffen sind, müssen hiervon nach § 613a Abs. 5 BGB in Textform unterrichtet werden. Die Information kann dabei durch den Veräußerer oder aber den Erwerber erfolgen, § 613a Abs. 5 BGB. Nach Zugang dieser Unterrichtung haben die betroffenen Beschäftigten einen Monat Zeit, dem Übergang ihres Arbeitsverhältnisses auf den Erwerber zu widersprechen, § 613a Abs. 6 BGB. Vereinbaren Veräußerer und Erwerber, dass der Letztere die betroffenen Beschäftigten nach § 613a Abs. 5 Alternative 2 BGB informieren soll, darf der Veräußerer bis zum Übergang des Betriebs- oder des Betriebsteils zunächst nur die erforderlichen Daten der Beschäftigten zur Abwicklung des Beschäftigungsverhältnisses an den Erwerber übermitteln, Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Eine Übermittlung von besonderen Kategorien personenbezogener Daten, wie zum Beispiel Arbeitsunfähigkeitsbescheinigungen als Personaldaten, ist hierfür nicht erforderlich.

- **Widerspruch der oder des Beschäftigten vor dem Betriebs-/Betriebsteilübergang**

  Soll die Information der betroffenen Beschäftigten – wie regelmäßig üblich – durch den Veräußerer nach § 613a Abs. 5 Alternative 1 BGB erfolgen und widersprechen betroffene Beschäftigte bevor der Betrieb oder der Betriebsteil auf den Erwerber übergegangen ist, ist eine Übermittlung der Daten der widersprechenden Beschäftigten durch den Veräußerer auf den Erwerber nicht erforderlich und damit unzulässig.

- **Kein Betriebs- oder Betriebsteilübergang nach § 613a BGB**

  Liegt ein Asset-Deal vor, der keinen Betriebs- oder Betriebsteilübergang nach § 613a BGB darstellt, sind für eine Übermittlung von Beschäftigtendaten individuelle Vereinbarungen zwischen Veräußerer, Erwerber und Beschäftigten zu treffen. Auch in diesen Fällen wird eine Übermittlung von Beschäftigtendaten regelmäßig nur mit einer freiwilligen und damit rechtswirksamen Einwilligung der betroffenen Beschäftigten möglich sein.[9]

V. Sonstige Hinweise

1. Bei allen Fallgruppen ist zu beachten:

- Die datenschutzrechtliche Verantwortung für die Übermittlung personenbezogener Daten an den Erwerber trifft den Veräußerer. Insbesondere muss der Veräußerer neben der Erfüllung der vorstehenden Anforderungen bei der Übermittlung ein angemessenes Schutzniveau gem. Art. 32 DS-GVO gewährleisten. Verarbeitet

9 Wegen der weiteren Einzelheiten zu einer rechtswirksamen Einwilligung wird auf die Ausführungen in der Fußnote 4 verwiesen

der Veräußerer weiterhin personenbezogene Daten seiner Kundinnen und Kunden (einschließlich des Falles, dass er den Erwerber als Auftragsverarbeiter einsetzt), ist er insoweit weiterhin für die Einhaltung seiner datenschutzrechtlichen Pflichten verantwortlich. Die Daten der Kundinnen und Kunden sind zu löschen, wenn die Voraussetzungen des Art. 17 DS-GVO vorliegen, es sei denn, Art. 17 Abs. 3 DS-GVO ist einschlägig (z. B. bei handels- oder steuerrechtlichen Aufbewahrungsfristen).

- Die datenschutzrechtliche Verantwortung für die Verarbeitung beim Erwerber trifft diesen. Der Erwerber muss die Pflichten als „Verantwortlicher" (Art. 4 Nr. 7 DS-GVO) erfüllen, soweit er nicht als Auftragsverarbeiter für den Veräußerer tätig ist. Unter anderem muss er ein angemessenes Schutzniveau gewährleisten und bei Vorliegen der entsprechenden Voraussetzungen die Betroffenenrechte erfüllen.

- Soweit die Voraussetzungen von Art. 14 Abs. 5 DS-GVO nicht vorliegen, muss der Erwerber, innerhalb einer angemessenen Frist, spätestens innerhalb eines Monats nach Erhalt der Datensätze vom Veräußerer, die Kundinnen und Kunden gem. Art. 14 DS-GVO informieren, insbesondere hat er sie auch nach Art. 14 Abs. 2 Buchst. c DS-GVO auf ihr Widerspruchsrecht nach Art. 21 DS-GVO hinzuweisen. Ein Widerspruch wirkt sich nur auf die Datenverarbeitung nach dem Zeitpunkt des Widerspruchs aus.

2. Übermittlung von Daten der Kundinnen und Kunden als einziges „Asset"

Eine Übermittlung im Rahmen eines Verkaufs von Daten der Kundinnen und Kunden als losgelöstes „Asset" (Verkauf von Kundendatenbanken) ist regelmäßig nur mit vorheriger Einwilligung der betroffenen Kundinnen und Kunden möglich. Dies gilt insbesondere dann, wenn die Datenbanken zur Werbung für Geschäftstätigkeiten genutzt werden soll, die in keinem Zusammenhang mit dem ursprünglichen Unternehmen stehen.

Nur wenn Kleinstunternehmen (weniger als 10 Beschäftigte) oder Kleinunternehmen (weniger als 50 Beschäftigte und ein Jahresumsatz von höchstens 10 Mio. Euro)[10] aufgrund der Beendigung der eigenen wirtschaftlichen Tätigkeit untereinander die Daten ihrer Kundinnen und Kunden einem Kleinst- oder Kleinunternehmen desselben Wirtschaftszweigs[11] übergeben, kann ausnahmsweise die einmalige Übermittlung ausschließlich der Postadressen im Wege einer Widerspruchslösung realisiert werden (z.B. der schließende Malerbetrieb A übergibt die Kundenadressen an einen bestehenden Malerbetrieb B, der aber weder Ausrüstung von Betrieb A übernimmt, noch in laufende Geschäftsbeziehungen eintritt).

---

10 Definition des Statistischen Bundesamts.
11 Nach den Festlegungen des Statistischen Bundesamts.

Über die Übertragung ihrer Postadressen werden in diesem Fall die betroffenen Kundinnen und Kunden vom Veräußerer unterrichtet und ihnen wird mitgeteilt, dass sie innerhalb einer angemessenen Frist (i.d.R. 4 – 6 Wochen) formlos gegenüber dem Veräußerer widersprechen können. Im Falle des Ausbleibens eines Widerspruchs kann die Übermittlung der Postadressen als einziges Asset ausnahmsweise auf Art. 6 Abs. 1 UAbs.1 Buchst. f DS-GVO gestützt werden. Diese Abwägung kann darauf gestützt werden, dass entsprechend Erwägungsgrund 13 Satz 4 der DS-GVO den Interessen der Kleinst- und Kleinunternehmen wegen der engen Kundenbeziehung und des besonderen Interesses an einer wirtschaftlich tragfähigen Regelung der Unternehmensnachfolge regelmäßig erhöhtes Gewicht zukommt und dem Schutz der Erwartungen und Interessen der Betroffenen durch ein voraussetzungsloses Widerspruchsrecht Rechnung getragen wird. Dem Veräußerer bleibt es unbenommen, Einwilligungen seiner bisherigen Kundinnen und Kunden auch zur Übermittlung von Telefonnummern und E-Mail-Adressen einzuholen.

11.09.2024 – DS-GVO privilegiert wissenschaftliche Forschung Positionspapier zum Begriff „wissenschaftliche Forschungszwecke”

Viele Regelungen der Datenschutz-Grundverordnung (DS-GVO) beziehen sich auf den Begriff der „wissenschaftlichen Forschungszwecke”. Hierzu zählen Art. 5 Abs. 1 Buchst. b DS-GVO (Zweckbindung), Art. 9 Abs. 2 Buchst. j DS-GVO (Öffnungsklausel für die Verarbeitung besonderer Kategorien personenbezogener Daten), Art. 14 Abs. 5 Buchst. b DS-GVO (Einschränkung der Informationspflichten), Art. 17 Abs. 3 Buchst. d DS-GVO (Einschränkung des Rechts auf Löschung), Art. 21 Abs. 6 DS-GVO (Widerspruchsrecht) und Art. 89 DS-GVO (besondere Garantien und Ausnahmen). Diese Regelungen privilegieren Datenverarbeitungen zu wissenschaftlichen Forschungszwecken und sehen bestimmte Ausnahmen und Einschränkungen von datenschutzrechtlichen Anforderungen vor.

Um festzustellen, ob diese privilegierenden Regelungen anwendbar sind, muss geprüft werden, ob eine Verarbeitung tatsächlich zu wissenschaftlichen Forschungszwecken erfolgt. Dies kann regelmäßig nur in einer Einzelfallbeurteilung erfolgen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder möchte mit den folgenden Kriterien eine Hilfestellung bei dieser Beurteilung geben.

Auf europäischer Ebene entwirft der Europäische Datenschutzausschuss (EDSA) derzeit Leitlinien zur wissenschaftlichen Forschung. Sofern diese Leitlinien weitergehende oder ergänzende Kriterien vorsehen werden, werden diese zusätzlich zu beachten sein.

Nach Erwägungsgrund 159 S. 2 DS-GVO soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne der DS-GVO weit ausgelegt werden und die technologische Entwicklung und Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Zugleich soll diese Forschung nach Erwägungsgrund 159 S. 3 DS-GVO den festgelegten Zielen aus Art. 179 Abs. 1 AEUV Rechnung tragen, was den sozialen Fortschritt, ein ausgewogenes Wirtschaftswachstum, die Verbesserung der Lebensqualität und Themen der öffentlichen Daseinsvorsorge umfasst.[12] Damit schließt das Verfolgen begleitender wirtschaftlicher Motive nicht die wissenschaftliche Forschung im Sinne der DS-GVO aus, solange die Tätigkeit auf Erzielung eines gesellschaftlichen Nutzens gerichtet ist.

Bei der Auslegung des Begriffes der wissenschaftlichen Forschung sind die Bestimmungen der Europäischen Grundrechtecharta (GRCh) zu berücksichtigen. Die Regelungen der DS-GVO dienen dem Schutz des Grundrechts auf Datenschutz nach Art. 8 GRCh[13] unter Berücksichtigung der übrigen Grundrechte;[14] die forschungsbezogenen Regelungen der DS-GVO sollen den Ausgleich mit der Forschungsfreiheit nach Art. 13 GRCh gewährleisten. Maßgaben für die gesetzliche Ausgestaltung der Grundrechte ergeben sich aus Art. 52 GRCh, wonach Einschränkungen unter Wahrung des Verhältnismäßigkeitsgrundsatzes nur zulässig sind, wenn sie den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen entsprechen oder dem Schutz der Rechte und Freiheiten anderer dienen. Diese Maßgaben sind bei Auslegung und Anwendung der Regelungen so zu berücksichtigen, dass die kollidierenden Grundrechte unter Achtung ihres Wesensgehaltes miteinander in Einklang gebracht werden.[15]

Der EuGH hat sich bisher nur am Rande zur Forschungsfreiheit geäußert.[16] Bei der unionsrechtsautonomen Auslegung ist Art. 13 GRCh zu berücksichtigen. Da Art. 13 GRCh allerdings als vom deutschen Grundgesetz „inspiriert" gilt, kann die Rechtsprechung des Bundesverfassungsgerichts[17] zu einem gewissen Grad auch zur Auslegung von Art. 13 GRCh herangezogen werden.[18] Als Forschung gilt nach der Rechtsprechung des Bundesverfassungsgerichts und der Kommentarliteratur zu Art. 13 GRCh

---

12 vgl. Grabitz/Hilf/Nettesheim/Eikenberg AEUV Art. 179 Rn. 30 f
13 Vgl. Jarass, Charta der Grundrechte der EU Art. 8 Rn 19.
14 Art. 1 DS-GVO und Erwägungsgrund 4, der allerdings in seiner nicht abschließenden Aufzählung der von der DSGVO geachtet Freiheiten und Grundsätze die Forschungsfreiheit nicht ausdrücklich erwähnt
15 Jarass, Charta der Grundrechte der EU Art. 52 Rn 43 m.w.N.
16 Roßnagel, ZD 2019, 157, 158 m. w. N.; im Zusammenhang mit Zollbestimmungen findet sich außerdem im Urteil vom 29.01.1985 (C-234/83, Gesamthochschule Duisburg) der Befund, dass mit "dem Begriff „wissenschaftliche Arbeiten", der sich auf die zu nicht kommerziellen Zwecken betriebene Forschung bezieht, (...)die Erlangung und Vertiefung wissenschaftlicher Erkenntnisse gemeint" sei.
17 vgl. z. B. BVerfG, BVerfGE 35, 79, 112 f.; BVerfGE 47, 327, 367.
18 Roßnagel, ZD 2019, 157, 158.

jede geistige Tätigkeit mit dem Ziel, in methodischer, systematischer sowie nachprüfbarer Art und Weise neue Erkenntnisse zu gewinnen.[19]

Der Begriff der Forschung ist personen- und institutionsunabhängig und umfasst auch die Ressort- und Industrieforschung, soweit diese die Forschungsfreiheit in Anspruch nehmen kann.[20]

Damit die privilegierenden Vorschriften der DS-GVO für die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung zur Anwendung kommen, müssen nach Feststellung der DSK folgende Kriterien erfüllt sein:

I. Methodisches und systematisches Vorgehen
Wissenschaftliche Forschung verlangt eine methodische und systematische Vorgehensweise.[21] Dabei sind fachspezifische Eigenarten und Besonderheiten zur Ermittlung der rationalen Wahrheit zu berücksichtigen.

II. Erkenntnisgewinn
Ein weiteres Kriterium für Forschung ist nach der Rechtsprechung des BVerfG das mit dem jeweiligen

Die bloße Anwendung bereits gewonnener Erkenntnisse fällt demgegenüber ebenso wenig unter den Begriff der wissenschaftlichen Forschung wie der Einsatz wissenschaftlicher Methoden zu reinen Aufsichts-, Kontroll-Organisations- oder Werbezwecken.

III. Nachprüfbarkeit
Nach der Rechtsprechung des BVerfG ist auch das Kriterium der „Nachprüfbarkeit" wesentlich für wissenschaftliche Forschung.[22]

Eine Veröffentlichung (als Publikationen, Vorträge o.Ä.) der Forschungsergebnisse ist keine zwingende Voraussetzung wissenschaftlicher Forschung.

Gleichwohl dürfte eine auf Erkenntnisgewinnung gerichtete Tätigkeit dann aus dem Anwendungsbereich der Vorschriften der DS-GVO, die wissenschaftliche Forschung privilegieren, herausfallen, wenn bewusst eine Geheimhaltung der Ergebnisse beabsichtigt ist, um sie so systematisch einer Überprüfung durch die Fachgemeinschaft zu entziehen.

Denn grundsätzlich ist die Öffentlichkeit der Wissenschaft eine Funktionsbedingung für einen offenen wissenschaftlichen Diskurs. Die Öffentlichkeit

---

19 BVerfG, BVerfGE 35, 79; Artikel 13 GRCh: Jarass, Charta der Grundrechte der Europäischen Union, 4. Aufl. 2021, Art. 13 Rn. 8.
20 vgl. Maunz/Dürig, Stand: August 2023, Art. 5 Abs. 3 GG Rn. 102.
21 BVerfG, BVerfGE 35, 79.
22 BVerfG, BVerfGE 35, 79.

ermöglicht die kritische Auseinandersetzung mit der angewandten Forschungsmethode und den Forschungsergebnissen und die Überprüfbarkeit im Fachkreis (Peer Review).

Im Rahmen des Kriteriums der Nachprüfbarkeit wird man deshalb verlangen, dass die Durchführung und die Ergebnisse des Forschungsvorhabens nach wissenschaftlichen Standards dokumentiert werden und nicht von vornherein eine Geheimhaltungsabsicht der oben beschriebenen Art besteht.

Dabei ist zu berücksichtigen, dass einer Veröffentlichung im Einzelfall Betriebs- oder Geschäftsgeheimnisse oder andere schutzwürdige Geheimhaltungsinteressen entgegenstehen können.

Für die Öffentlichkeit kann es z. B. ausreichend sein, dass eine Erfindung patentiert wird.

IV. Unabhängigkeit und Selbstständigkeit

Wissenschaftliche Forschung erfordert Unabhängigkeit und Selbstständigkeit.[23] Die Forschungsfreiheit hat daher auch gegenüber Auftraggebern zu bestehen. Zwar kann die wissenschaftliche Arbeit weisungsbegleitet sein, sie muss gleichzeitig aber autonom möglich sein.[24]

Soweit Auftraggeber weisend Einfluss auf den Untersuchungsverlauf oder den Umgang mit erlangten Ergebnissen nehmen und den Forschenden damit Spielräume nehmen so dass ihre Unabhängigkeit gefährdet wird, wird man wohl regelmäßig nicht von einer forschenden Tätigkeit des Auftragnehmers ausgehen können.

Eine bloße Kritik des Auftraggebers an der Forschung des Auftragnehmers ist hingegen unschädlich.

V. Gemeinwohlinteresse

Ein weiteres sich auch aus Art. 52 Abs. 1 GRCh ergebendes Kriterium für wissenschaftliche Forschungszwecke im Sinne der DS-GVO sind der gesellschaftliche Nutzen bzw. die Gemeinwohleffekte des Vorhabens.

Die in der DS-GVO vorgesehenen Privilegierungen wissenschaftlicher Forschungszwecke und die entsprechenden Einschränkungen der Rechte betroffener Personen sind nur dadurch zu rechtfertigen, dass wissenschaftliche Forschung dem Gemeinwohl zugutekommt und nicht ausschließlich kommerziellen oder sonstigen Einzelinteressen dient.

---

23 Roßnagel, ZD 2019, 157, 158.
24 vgl. Maunz/Dürig, Stand: August 2023, Art. 5 Abs. 3 GG Rn. 102.

19.08.2024 – Positionspapier – Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)

In einigen Kommunen ist eine sog. Bezahlkarte für die Auszahlung von Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) bereits im Einsatz, in vielen anderen ist ihre Einführung in naher Zukunft vorgesehen. Auf Bund-Länder-Ebene wurden am 31. Januar 2024 bundeseinheitliche Mindeststandards1 beschlossen. Aus diesen geht hervor, wie die Bezahlkarte ausgestaltet werden und welche technischen Möglichkeiten sie bieten soll. Seit dem 16. Mai 2024 ist zudem eine Änderung des AsylbLG in Kraft, wonach die Leistungsgewährung in bestimmten Konstellationen auch mithilfe einer Bezahlkarte erfolgen kann.[25] Bei der Bezahlkarte handelt es sich um eine guthabenbasierte Karte mit Debit-Funktion, aber ohne Verknüpfung mit einem herkömmlichen Girokonto. Die Einführung der Bezahlkarte erfolgt in der Praxis unter Einbindung eines Dienstleisters in Gestalt eines privatrechtlichen Bankunternehmens. Durch diese Art der Leistungsgewährung sowie die avisierten weiteren Funktionsmöglichkeiten der Karte entstehen zwangsläufig datenschutzrechtlich relevante Verarbeitungsvorgänge der personenbezogenen Daten von Leistungsberechtigten. Damit wird in das Recht der Leistungsberechtigten auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG eingegriffen, welches im Lichte des Rechts auf den Schutz personenbezogener Daten nach Art. 8 Charta der Grundrechte der EU (GRCh) in Verbindung mit Art. 7 GRCh auszulegen ist.[26] Dieses Recht gilt gleichermaßen für deutsche wie ausländische Staatsangehörige, die sich in der Bundesrepublik Deutschland aufhalten. Aus dem Grundrecht folgen Bedingungen und Grenzen, die bei der Umsetzung der Leistungsgewährung mittels Bezahlkarten zu berücksichtigen sind.

I. Datenschutzrechtliche Zulässigkeit der Leistungsmethode „Bezahlkarte"

Der Bundesgesetzgeber hat die Bezahlkarte in den §§ 2, 3 und 11 AsylbLG als eine Methode zur Leistungserbringung nun ausdrücklich gesetzlich normiert.[27] Dabei hat der Gesetzgeber darauf verzichtet, eine spezifische Rechtsgrundlage für die in den Leistungsbehörden bei Umsetzung der Bezahlkarte nunmehr anfallenden Verarbeitungen von personenbezogenen Daten zu schaffen. Für diese Vorgänge wird jedoch eine Rechtsgrundlage benötigt, die den Anforderungen von Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO genügt. Deswegen hängt die datenschutzrechtliche Zulässigkeit

25 BGBl. 2024 I Nr. 152 vom 15.05.2024, S. 29 f.
26 Siehe zu diesem Grundrechtsverständnis BVerfG, Beschluss vom 6.11.2019 – 1 BvR 16/13 Rn. 46, 60 ff.
27 Siehe BT-Drucksache 20/1106.

der Leistungsmethode „Bezahlkarte" davon ab, ob ein Rückgriff auf die Generalklauseln des Landesdatenschutzrechts[28] erfolgen darf. Angesichts der in Bezug auf das Recht auf Schutz personenbezogener Daten hier als moderat zu bewertenden Eingriffsintensität ist dies prinzipiell möglich: Die behördliche Verarbeitungstätigkeit einschließlich der Datenweitergabe an den Dienstleister kann grundsätzlich auf die jeweilige landesdatenschutzrechtliche Generalklausel gestützt werden.[29]

Dies gilt allerdings nur, soweit ausschließlich die zur Leistungserbringung erforderlichen personenbezogenen Daten verarbeitet werden. Entscheidend für die Zulässigkeit der Verarbeitung personenbezogener Daten beim Einsatz der Bezahlkarte ist somit, welche Zwecke das AsylbLG fachrechtlich vorgibt und welche Verarbeitungsvorgänge zur Erreichung dieser Zwecke zwingend benötigt werden.

II. Datenschutzrechtliche Grenzen bei Umsetzung der Bezahlkarte

Die für Behörden geltenden rechtlichen Grenzen für die Verarbeitung von personenbezogenen Daten dürfen bei der Einbindung des privaten Zahlungsdienstleisters nicht überschritten werden. Insbesondere ist zu beachten, dass es gemäß Art. 6 Abs. 1 UAbs. 2 DSGVO Behörden selbst nicht gestattet ist, eine Datenverarbeitung unter Verweis auf ein überwiegendes berechtigtes Interesse gemäß Art. 6 Abs. 1 Buchst. f DSGVO durchzuführen. Diese Vorgabe des europäischen Gesetzgebers darf nicht durch eine Auslagerung der Datenverarbeitung an eine nichtöffentliche Stelle umgangen werden. Es wäre daher datenschutzrechtlich unzulässig, den Dienstleister – unter Verweis auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO – bestimmte Datenverarbeitungen im Interesse der Behördenvornehmen zu lassen, wenn die Behörde diese nicht selbst, gestützt auf eigene Rechtsgrundlagen, durchführen darf.

Wird also im Folgenden erläutert, dass ein angestrebter Verarbeitungsvorgang nicht von einer Leistungsbehörde ausgeführt werden darf, so gilt dies auch für den jeweiligen Dienstleister, soweit er die Verarbeitung lediglich für Leistungsbehörden durchführt.

1. Keine Einsichtnahme in den Guthabenstand

Eine eigenständige Einsichtnahme in den Guthabenstand von leistungsberechtigten Personen durch die Leistungsbehörden ist nach derzeitiger Rechtslage unzulässig. Ein solcher Abruf dieser Information ist eine Verarbeitung personenbezogener Daten, die eine Rechtsgrundlage be-

---

28 Siehe § 4 Abs. 1 BayDSG; § 5 Abs. 1 BbgDSG; § 3 BlnDSG; § 3 Abs. 1 BremDSGVOAG; § 4 DSAG LSA; § 4 Abs. 1 DSG M-V; § 3 DSG NRW; § 3 Abs. 1 HDSIG; § 4 HmbDSG; § 4 LDSG BW; § 3 LDSG RLP; § 3 Abs. 1 LDSG SH; § 3 NDSG; § 3 Abs. 1 SächsDSDG; § 4 Abs. 1 SDSG; § 16 Abs. 1 ThürDSG.

29 Von der Eingriffsintensität zu trennen ist die Risikobewertung, wie sie im Rahmen einer Datenschutz-Folgenabschätzung anhand der konkreten Funktionen der Bezahlkarte vorzunehmen ist.

nötigt. In Betracht käme hierfür einzig die o.g. datenschutzrechtliche Generalklausel nach dem jeweiligen Landesrecht. Deren Voraussetzung der Erforderlichkeit dieser Verarbeitung für die Gewährung der Leistungen nach dem AsylbLG ist jedoch nicht erfüllt.

Durch Einfügen des Wortes „Bezahlkarte" in die §§ 2, 3 und 11 AsylbLG hat der Gesetzgeber zwar deutlich gemacht, dass die zuständigen Behörden Leistungen durch den Einsatz einer guthabenbasierten Karte mit Debit-Funktion erbringen dürfen. Weder im Gesetzestext noch in der dazugehörigen Begründung findet sich jedoch ein Hinweis darauf, dass Leistungsbehörden Einsicht in den Guthabenstand nehmen dürfen.[30] Der Gesetzgeber hat gerade nicht vorgesehen, dass die Bezahlkarte den Leistungsbehörden ein Mehr an Informationen über die Leistungsberechtigten verschafft, als es bisher der Fall war. Eine vergleichbare Kontrollmöglichkeit bei der Ausgabe von Sachleistungen, Wertgutscheinen oder Bargeld existiert nicht. Dementsprechend würde durch eine Einsichtnahme-Funktion ein zusätzlicher Eingriff erfolgen, der geeignet ist, den betroffenen Leistungsberechtigten das Gefühl ständiger Überwachung zu vermitteln und der offenkundig nicht benötigt wird, um die Leistung zu gewähren.

Selbst wenn im Einzelfall eine Leistungsbehörde Kenntnis über einen Guthabenstand benötigt, etwa weil die leistungsberechtigte Person ihre Karte verloren hat und ein bestehendes Guthaben auf eine neue Karte übertragen werden soll, bedarf es keines technischen Direktzugriffs für die Behörde. Als milderes Mittel kann die leistungsberechtigte Person über die Mitwirkungspflichten nach § 9 Abs. 3 AsylbLG i.V.m. §§ 60 ff. SGB I dazu angehalten werden, der Behörde beispielsweise vor Ort an einem Behördencomputer die Einsicht in den Guthabenstand zu ermöglichen.

2. Keine pauschale Einschränkung auf Postleitzahlen-Gebiete

Für die räumliche Einschränkung der Einsatzmöglichkeit der Bezahlkarte muss die Information verarbeitet werden, dass für betroffene Leistungsberechtigte Aufenthaltsbeschränkungen bestehen. Diese Information stellt auch dann ein personenbezogenes Datum dar, wenn sie über die Karte nur mittelbar mit der leistungsberechtigten Person verknüpft wird. Denn jede Karte ist eindeutig einer nach dem AsylbLG leistungsberechtigten Person zugeordnet und würde im Falle einer räumlichen Einsatzbeschränkung zugleich die Information enthalten, inwiefern die betroffene Person in ihrer Freizügigkeit eingeschränkt ist, mithin asyl- oder aufenthaltsrechtlichen Beschränkungen unterliegt. Für die Verarbeitung dieser Information wird daher eine Rechtsgrundlage benötigt. Auch hier kommt allein die Generalklausel des jeweiligen Landesdatenschutzrechts in Betracht, da keine bereichsspezifischen Rechtsgrundlagen existieren.

30 Siehe BT-Drucksache 20/11006, S. 101 ff.

Die Voraussetzungen der Generalklausel(n) liegen jedoch in der Regel nicht vor. Der Verarbeitungsvorgang ist zur Leistungsgewährung grundsätzlich nicht erforderlich. Erforderlich kann nur eine Datenverarbeitung sein, die den Zweck der Leistungsgewährung gemäß dem AsylbLG verfolgt. Mit einer Beschränkung auf Postleitzahlengebiete werden jedoch über die Leistungsgewährung hinausgehende Zwecke verfolgt, namentlich die Durchsetzung räumlicher Aufenthaltsbeschränkungen nach dem Asyl- oder dem Aufenthaltsgesetz. Diese sind jedoch keine Voraussetzung für die Bewilligung von Grundleistungen nach den für die Bezahlkarte maßgeblichen Regelungen (§ 2 Abs. 2, § 3 Abs. 2, 3 u. 5 AsylbLG). Zum Zeitpunkt der Bewilligungsentscheidung fehlt es daher grundsätzlich an dem notwendigen fachrechtlichen Anknüpfungspunkt und somit an der Erforderlichkeit der Datenverarbeitung.[31]

Dies steht auch im Einklang mit § 11 Abs. 2 AsylbLG, der eine Verbindung zwischen dem Leistungsbezug und der Verletzung räumlicher Aufenthalts- und Wohnsitzpflichten herstellt. Das Vorliegen einer solchen Verletzung muss allerdings zunächst im Einzelfall festgestellt werden, bevor auf der Grundlage von § 11 Abs. 2 AsylbLG Leistungsbeschränkungen erfolgen dürfen. Dies ist schon deswegen geboten, weil ein Aufenthalt außerhalb des zugewiesenen Bereichs nicht zwingend gegen räumliche Beschränkungen verstößt, wie sich etwa aus den Möglichkeiten nach § 12 Abs. 5 AufenthG sowie § 57 AsylG zum rechtskonformen Verlassen des Aufenthaltsbereichs ergibt. Anders verhält es sich im Übrigen mit einer Einschränkung der Einsatzmöglichkeit der Bezahlkarte auf das Bundesgebiet. Der Aufenthalt im Bundesgebiet ist gemäß § 1 Abs. 1 Hs. 1 AsylbLG Voraussetzung für die Leistungsberechtigung. Diesbezüglich besteht folglich ein unmittelbarer Bezug zwischen dem Zweck des AsylbLG und der Datenverarbeitung, sodass die mit dieser Einschränkung einhergehende Datenverarbeitung keinen datenschutzrechtlichen Bedenken begegnet.

3. Trennung der Datensätze

Für den praktischen Einsatz von Bezahlkarten muss die Verwaltung auf einen Dienstleister zugreifen, der die Durchführung aller Transaktionen auf Bankebene übernimmt. Ist ein Dienstleister leistungsbehördenübergreifend tätig, werden durch ihn die Datensätze einer Vielzahl von Verantwortlichen verarbeitet. Es darf dadurch aber nicht dazu kommen, dass ein behördenübergreifendes Register auf Seiten des Dienstleisters entsteht. Denn in Gestalt des Ausländerzentralregisters existiert bereits ein bundesweites Register aller Personen mit ausländischer Staatsangehörigkeit mit dem Ziel, durch eine zentrale Datenhaltung divergierende ausländer- oder asylrechtliche Entscheidungen zur gleichen Person zu vermeiden. Es besteht folglich zur Erreichung dieses Zwecks kein

31 Das Erfordernis eines fachrechtlichen Anknüpfungspunkts führt i.Ü. dazu, dass auch sonstige, dem AsylbLG fremde Zwecke nicht berücksichtigt werden dürfen, um eine PLZ-Beschränkung zu begründen. Dies gilt beispielsweise für die Erwägung, Kaufkraft innerhalb der jeweiligen Kommune halten zu wollen.

Bedarf für ein weiteres Register. Insbesondere ist noch auf Folgendes hinzuweisen:

a) Angemessene technische und organisatorische Maßnahmen, insbesondere: Mandantentrennung

Mit Blick auf die Verpflichtung zur Gewährleistung der Sicherheit der Datenverarbeitung, Art. 32 DSGVO, ist zudem durch eine Mandantentrennung auf Seiten des Dienstleisters die Integrität und Vertraulichkeit der Daten der jeweiligen Leistungsbehörde sicherzustellen.

b) Kein behördenübergreifender Datenabgleich außerhalb der behördlichen Befugnisse

Die bei einem Dienstleister zusammenfallenden Datenbestände mehrerer Behörden dürfen nach derzeitiger Rechtslage zudem nicht durch diesen abgeglichen werden. Für einen solchen Datenabgleich beim Dienstleister steht keine Rechtsgrundlage zur Verfügung. Die spezialgesetzlichen Regelungen des Ausländerzentralregistergesetzes (AZRG) versperren den Zugriff auf datenschutzrechtliche Generalklauseln.

Überdies ergibt sich kein Mehrwert durch einen solchen Datenabgleich, insbesondere nicht hinsichtlich der Ermittlung eines etwaigen Leistungsmissbrauchs. Der Einsatz der Bezahlkarte ist eine Methode der Leistungsgewährung. Vor der Kartenausgabe, mithin auch vor der Weitergabe der Daten der Asylbewerber:innen an den Dienstleister, muss die Leistungsbehörde deren Leistungsberechtigung ohnehin prüfen. Bezöge die jeweilige Person bereits an anderer Stelle Leistungen, so würde sich dies aus dem Ausländerzentralregister ergeben. Ein Mehr an Erkenntnis könnte der Dienstleister nicht ermitteln. Vielmehr entstünde durch einen solchen Abgleich eine Parallelstruktur ohne erkennbaren Nutzen, dafür mit erheblichen Risiken für die Betroffenen und mit Blick auf die Datenrichtigkeit auch für die öffentlichen Stellen.

4. Keine Weitergabe der Ausländerzentralregister-Nummer an den Dienstleister

Nach gegenwärtiger Rechtslage ist eine Weitergabe der Ausländerzentralregister-Nummer (AZR-Nummer) an den Dienstleister rechtswidrig.

Die Übermittlung der AZR-Nummer an eine nicht-öffentliche Stelle sehen weder das AZRG noch die AZRG-Durchführungsverordnung für mit der hiesigen Konstellation vergleichbare Fälle vor. Die nach den §§ 25 und 27 AZRG zulässigen Übermittlungen von Informationen aus dem AZR an nicht-öffentliche Stellen sind nicht einschlägig.

Ferner ergibt sich aus § 10 Abs. 4 AZRG, dass die AZR-Nummer grundsätzlich nur im Verkehr mit dem vom Bundesamt für Migration und Flüchtlinge

(BAMF) geführten Ausländerzentralregister genutzt werden darf. Zwar bestehen Ausnahmen nach § 10 Abs. 4 S. 2 AZRG. Diese beinhalten jedoch keine Weitergabe der AZR-Nummer an nicht-öffentliche Stellen.

Angesichts der abschließenden, spezialgesetzlichen Regelungen des AZRG ist der Rückgriff auf die datenschutzrechtlichen Generalklauseln gesperrt. Im Übrigen würde es auch hier an der Erforderlichkeit in Bezug auf die Verfügbarkeit der AZR-Nummer für den Dienstleister fehlen (vgl. Nr. 3.b): Es ist Aufgabe der Leistungsbehörden, die Leistungsberechtigung einer Person festzustellen. Zu diesem Zweck werden diesen Daten aus dem Ausländerzentralregister zur Verfügung gestellt, § 18a AZRG. Nach Feststellung der Leistungsberechtigung wird der Bezahlkarten-Dienstleister zur Ausführung dieser Entscheidung herangezogen. Ein dann stattfindender Abgleich der AZR-Nummer kann gegenüber der bereits erfolgten Prüfung keine neuen Erkenntnisse liefern und ist daher auch nicht erforderlich.

5. Zugriff der Sicherheitsbehörden auf Buchungsdaten
Infolge der Nutzung der Bezahlkarte werden personenbezogene Daten der leistungsberechtigten Personen erhoben und gespeichert, die erheblichen Aufschluss über die private Lebensgestaltung geben können. Zugriffe durch Sicherheitsbehörden dürfen vor diesem Hintergrund nur nach den gesetzlichen Maßgaben der einschlägigen Sicherheitsgesetze, z.B. der Strafprozessordnung erfolgen, die auch für andere Personen und deren Bankaktivitäten gelten.

15. Mai 2024 – Positionspapier – Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken

„Genetische Daten" sind nach Artikel 4 Nummer 13 der Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

Die Nutzung genetischer Daten ist die Grundlage für eine personalisierte, auf die individuelle Patientin oder den individuellen Patienten angepasste Präzisionsmedizin. Die Forschung mit genetischen Daten kann den biomedizinischen Fortschritt wesentlich voranbringen und zu einer verbesserten medizinischen Versorgung beitragen.[32] Insbesondere in

32 Vgl. z. B. https://www.gesundheitsforschung-bmbf.de/de/medizinische-genomforschung-6640.php.

der Krebsforschung und der Erforschung seltener Erkrankungen kann die Analyse genetischer Daten zu vielversprechenden Behandlungs- oder sogar Heilungsmöglichkeiten führen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert daher eine datenschutzkonforme wissenschaftliche biomedizinische Forschung mit genetischen Daten zum Wohle der Patientinnen und Patienten, indem dazu ein gesetzlicher Rahmen geschaffen wird, der sanktionsbewehrte hohe Schutz- und Vertrauensanforderungen und wirksame Mitwirkungs- und Kontrollmöglichkeiten der betroffenen Personen vorsieht.

Forschung mit körpereigenen Substanzen, wie z. B. Blut, Haaren oder Speichel, die ohne Kenntnis der betroffenen Person erlangt wurden, muss verboten bleiben.

I. Besonders hohe Risiken

Genetische Daten sind von äußerster Sensibilität und bergen ein „hohes prädiktives Potential" mit Blick auf die betroffene Person und biologische Verwandte. Aus genetischen Daten lassen sich unter anderem Erkenntnisse über gesundheitliche Prädispositionen, Gesundheitsrisiken und vererbliche Erkrankungen ableiten. Diese Erkenntnisse betreffen nicht nur die betroffene Person selbst, sondern können sich auch auf leibliche Familienangehörige erstrecken. Anhand der Analyse genetischer Daten lassen sich damit Wahrscheinlichkeitsaussagen über das Auftreten von Krankheiten der leiblich miteinander verwandten Personen treffen.

Das Diskriminierungs- und Stigmatisierungsrisiko bei Kenntnis dieser Daten, z. B. durch Versicherungen und Arbeitgeber, ist daher enorm. Risikoerhöhend wirkt sich außerdem die Tatsache aus, dass genetische Daten durch die betroffenen Personen nicht verändert werden können, sondern diesen ihr Leben lang und auch darüber hinaus anhaften.

Die Weiterverarbeitung genetischer Daten in der medizinischen Sekundärnutzung (insbesondere zur Forschung) betrifft daher aufgrund von Rückschlüssen auf persönlichkeitsrelevante Merkmale wie Erbanlagen und (potentielle) Krankheiten regelmäßig den absolut geschützten Kernbereich der Persönlichkeit.

In diesem Zusammenhang muss zudem berücksichtigt werden, dass eine wirksame Anonymisierung genetischer Daten in der Regel daran scheitert, dass – etwa über einen Abgleich mit anderen genetischen Daten der betroffenen Person – eine Identifizierung möglich ist. Der Personenbezug lässt sich daher aus genetischen Daten in der Regel nicht entfernen. Genetische Daten sind deshalb schon aufgrund ihres potentiellen Informationsgehalts regelmäßig als personenbezogene Daten zu behandeln.

II. Besondere Regeln: ausdrückliche Einwilligung
Aus diesen Gründen muss der Umgang mit genetischen Daten qualifizierten datenschutzrechtlichen Regeln unterliegen, die die Rechte und Freiheiten der betroffenen Person in ausreichendem Maße wahren.

Für die datenschutzkonforme Verarbeitung genetischer Daten bedarf es daher grundsätzlich der ausdrücklichen Einwilligung der betroffenen Personen. Denn gerade in diesem äußerst sensiblen Bereich vermag nur die datenschutzrechtliche Einwilligung als Grundlage für eine individuelle Rechtsausübung dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen.[33]

Die DSK hat bereits 2001 auf die besondere Sensibilität genetischer Daten hingewiesen und eine gesetzliche Regelung von genetischen Untersuchungen gefordert.[34] Mit dem Gendiagnostikgesetz (GenDG) wurde eine solche gesetzliche Regelung zum 1. Februar 2010 geschaffen. Zu Recht bestimmt das Gendiagnostikgesetz, dass bei genetischen Untersuchungen oder Analysen eine Verarbeitung genetischer Daten nur mit ausdrücklicher und schriftlicher Einwilligung der betroffenen Personen erfolgen darf.

Das Gendiagnostikgesetz gilt aber ausdrücklich nicht für die Verarbeitung von Daten zu Forschungszwecken (§ 2 Absatz 2 Nr. 1 GenDG). Für die Verarbeitung genetischer Daten zu Forschungszwecken gelten bislang deshalb lediglich die allgemeinen Regelungen für die Forschung mit besonderen Kategorien personenbezogener Daten.

Die wirksame informierte, freiwillige und ausdrückliche Einwilligung der betroffenen Personen allein ist aber im absolut geschützten Kernbereich der Persönlichkeit noch kein ausreichender Schutzgarant des Rechts auf informationelle Selbstbestimmung. Vielmehr muss bei jeglicher Verarbeitung genetischer Daten im Rahmen einer Sekundärnutzung zu Forschungszwecken zusätzlich sichergestellt sein, dass erforderliche angemessene und spezifische Garantien und technische sowie organisatorische Schutzmaßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorgeschrieben sind und einer regelmäßigen Prüfung und Aktualisierung unterliegen.

Im Bereich der genetischen Forschung ist ein vielfältiger Datenaustausch und die Vernetzung der genetischen Datenbestände das erklärte Ziel vieler Vorhaben. Häufig können zum Zeitpunkt der Informationsbereitstellung die Zwecke der Verarbeitung bezogen auf konkrete Forschungsprojekte im

33 DSK: Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022, S. 5, https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.
34 DSK-Entschließung zur „Gesetzlichen Regelung von genetischen Untersuchungen" vom 24.10.2001, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/62DSK-GesetzlicheRegelungVonGenetischenUntersuchungen.pdf.

Einzelnen noch nicht vollständig und präzise angegeben werden, sodass die Einwilligung mangels ausreichender Bestimmtheit möglicherweise an rechtliche Grenzen stößt. Die Nutzung einer breiten Einwilligung (Broad Consent) im Sinne des Erwägungsgrunds 33 DS-GVO zur Verarbeitung genetischer Daten kann hier eine Lösung bieten. Jedoch sollten auch die Anforderungen und Grenzen der breiten Einwilligung gesetzlich geregelt werden, um die hier bestehende Rechtsunsicherheit zu beseitigen. Außerdem müssen zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz, Vertrauensbildung, Partizipation und Datensicherheit getroffen werden.[35]

Die Notwendigkeit der ausdrücklichen Einwilligung für die Sekundärnutzung zu Forschungszwecken ergibt sich schon daraus, dass die Erhebung der genetischen Probe und die genetische Untersuchung selbst nach Artikel 3 Absatz 2 Buchst. a EU-Grundrechte-Charta und dem Gendiagnostikgesetz einer Einwilligung bedürfen. Es wäre daher treuwidrig, entgegen der eingeholten Einwilligung die genetischen Daten auch für andere Zwecke zu verarbeiten (Artikel 5 Absatz 1 Buchst. a und b DS-GVO).

Sowohl bei einer spezifischen Einwilligung als auch bei der breiten Einwilligung darf es im besonders sensiblen Bereich der Sekundärnutzung genetischer Daten nicht den Verantwortlichen überlassen werden, welche flankierenden technischen und organisatorischen Schutzmaßnahmen zu treffen sind. Stattdessen bedarf es gesetzlicher Vorgaben über das zu realisierende hohe Schutz- und Vertrauensniveau, gerade auch mit Blick auf die Mitbetroffenheit von biologischen Verwandten.

Die DSK ist aufgrund der genannten Erwägungen der Auffassung, dass für die Sekundärnutzung genetischer Daten zu Forschungszwecken eine differenzierte und rechtsklare gesetzliche Regelung geschaffen werden muss, um das Interesse an der wissenschaftlichen Nutzung genetischer Daten mit dem Recht auf informationelle Selbstbestimmung und dem Recht auf Nichtwissen im hier betroffenen, absolut geschützten Kernbereich der Persönlichkeit in Einklang zu bringen.

Artikel 9 Absatz 4 DS-GVO wie auch voraussichtlich die EHDS-Verordnung sehen ausdrücklich eine entsprechende Öffnungsklausel für zusätzliche Bedingungen, einschließlich Beschränkungen, zur Verarbeitung genetischer Daten vor.

III. Besonders hohe Schutzmaßnahmen
In einer solchen gesetzlichen Regelung zur Sekundärnutzung genetischer Daten zu Forschungszwecken sollte die ausdrückliche Einwilligung als notwendige Voraussetzung der Verarbeitung vorgesehen werden. Gleich-

---

35 Vgl. Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO vom 03.04.2019, https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.

zeitig ist durch wirksame technische und organisatorische Garantien im Sinne der Konzepte des „data protection by design" und „data protection by default" sicherzustellen, dass nach einem Widerruf der Einwilligung die Verarbeitung der genetischen Daten der betroffenen Personen endet und die Betroffenenrechte stets wirksam ausgeübt werden können.

Die gesetzliche Regelung sollte zudem zwischen den verschiedenen Verarbeitungszwecken der Sekundärnutzung, wie der Forschung und der Qualitätssicherung, differenzieren. Bei dieser Differenzierung ist auch zu berücksichtigen, dass Erwägungsgrund 33 DS-GVO die Möglichkeit der breiten Einwilligung nur für die wissenschaftliche Forschung und nicht für die Qualitätssicherung eröffnet.

Eine gesetzliche Regelung über die Verarbeitung genetischer Daten zur Sekundärnutzung sollte im Hinblick auf die Grundsätze der Zweckbindung und Datenminimierung (Artikel 5 Absatz 1 Buchst. b und c DS-GVO) außerdem widerspiegeln, dass eine Qualitätssicherung und Evaluation der medizinischen Nutzung genetischer Daten die Verarbeitung nur legitimieren kann, wenn die Ziele der zu sichernden Qualität bzw. die Zwecke der Evaluation genau bestimmt sind und solange und soweit die Verarbeitung für diese Zwecke zwingend erforderlich ist.

Zudem hält es die DSK für geboten, dass eine gesetzliche Regelung für die Verarbeitung genetischer Daten zu Zwecken der Sekundärnutzung besondere Schutzmaßnahmen vorsieht. Dabei sollte insbesondere Folgendes gewährleistet werden:

- Verpflichtung zur Einhaltung einer Mindestbedenkzeit zwischen Informationsbereitstellung und Abgabe einer Einwilligungserklärung i. V. m. Hilfsangeboten für betroffene Personen und deren Angehörige (z. B. psychosoziale Beratung).

- Aufklärung und Beratung für die Entscheidung der betroffenen Personen über den Umgang mit individuell relevanten Forschungsergebnissen und Zufallsbefunden („Recht auf Nichtwissen") nach Information über mögliche Risiken und Auswirkungen der Kenntnisnahme für die betroffene Person und den biologisch Verwandten sowie Hinweis auf die Möglichkeit zur Änderung dieser Entscheidung.

- Transparenz der Datenverarbeitung durch Festlegung umfassender Informations- und Aufklärungspflichten zu Zwecken, Reichweite und Risiken der Verarbeitung für die Rechte und Freiheiten natürlicher Personen.

- Erweiterte Kontroll- und Mitwirkungsmöglichkeiten für betroffene Personen, z. B. durch aktive, rechtzeitige und leicht zugängliche Bereitstellung aktueller Informationen über neue Forschungsvor-

haben und barrierefreie Ausübung von Widerrufsrechten und Betroffenenrechten über digitale Managementsysteme.[36]

- Genehmigungspflicht von Forschungsvorhaben durch eine Ethikkommission.

- Die Rechtsgrundlage einer breiten Einwilligung ist nur unter strengen Vorgaben zulässig: Es bedarf spezifischer Aufklärungs- und Beratungsanforderungen und einer zeitlichen Begrenzung der Gültigkeit von Einwilligungen.

- Verschlüsselte Verarbeitung genetischer Daten und frühestmögliche Pseudonymisierung unter Einbindung unabhängiger Vertrauensstellen ggf. i. V. m. weiteren standardisierten Vorgaben zu den technischen und organisatorischen Maßnahmen einschließlich der Sicherheitsmaßnahmen und technisch implementierten Speicherbegrenzung und Löschung.[37]

- Lösch- und Vernichtungspflichten für die genetischen Daten und biologischen Proben mit einer gesetzlich festgelegten Aufbewahrungsdauer.

- Festlegung spezifischer sanktionsbewehrter Offenlegungs- und Übermittlungsverbote, insbesondere an Arbeitgeber oder Versicherungen und Strafbarkeit missbräuchlicher, zweck- und gesetzwidriger Nutzung genetischer Daten. Ein effektiver Schutz gegen die Beschaffung und Verwendung genetischer Proben ohne Kenntnis der betroffenen Personen sollte strafrechtlich geregelt werden.

- Zugang zu genetischen Daten von berechtigten Dritten nur nach einem Use & Access-Verfahren, das auch die datenschutzrechtlichen Grundsätze wie die Beschränkung des Zugangs für einen bestimmten wissenschaftlichen Forschungszweck, für eine bestimmte Zeit und für qualifizierte Forscherinnen und Forscher umfasst. Ein Datenzugriff berechtigter Dritter ist im Rahmen einer sicheren Verarbeitungsumgebung zu gewähren.

- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.

- Besonderer Schutz von Ungeborenen, Minderjährigen und nicht einwilligungsfähigen Personen, beispielsweise durch die Beschränkung bestimmter Forschungsziele sowie durch spezifische Aufklärung und Informationsbereitstellung für die gesetzlichen Vertreter (u. a. Personensorgeberechtigte, Vormunde, Betreuer).

---

36 Petersberger Erklärung und Beschluss der DSK vom 27.04.2020, abrufbar unter: https://datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf.
37 Arbeitspapier über genetische Daten, Artikel 29-Datenschutzgruppe, 12178/03/DE, 17.03.2004, S. 12.

- Vorgaben zur Wahrung der Anonymität der betroffenen Personen bei Publikation von Forschungsergebnissen.

Die DSK hat in ihrer Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken" vom 23.11.2023 weitere angemessene und spezifische Maßnahmen für eine gesetzliche Regelung zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken dargestellt, die zudem beachtet werden müssen.[38]

03.05.2024 – Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KIVO) – Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. Mai 2024

Die KI-VO sieht bereits in einigen Fällen die sektorspezifische Zuständigkeit der Datenschutzbehörden als Marktüberwachungsbehörden vor. Aufgrund ihrer bestehenden Zuständigkeiten nach der DSGVO, ihrer langjährigen Expertise im digitalen Grundrechtsschutz und etablierten, kooperativen Aufsichts- sowie Abstimmungsmechanismen sollte diese Kompetenz ausgeweitet werden. Die Datenschutzaufsichtsbehörden sind bereit, die Aufgabe der nationalen Marktüberwachung für KI-Systeme zu übernehmen.

Im März 2024 hat das Europäische Parlament die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz angenommen. Nach Inkrafttreten der KI-VO muss in Deutschland innerhalb von 12 Monaten eine behördliche Aufsichtsstruktur eingerichtet werden. Damit besteht Handlungsbedarf für die Gesetzgeber in Bund und Ländern.

Aufgrund der bereits jetzt durch die DSGVO begründeten Aufgaben und Befugnisse der Datenschutzaufsichtsbehörden sowie der langjährigen Erfahrung im Bereich der Beratung, Beschwerdebearbeitung und Kooperation auf nationaler wie europäischer Ebene sollten in Deutschland grundsätzlich die nationalen Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden benannt werden. Das Ziel einer einheitlichen

38 DSK-Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken" vom 23.11.2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf.

Anwendung der KI-VO wäre mit der Einrichtung weiterer Marktüberwachungsbehörden kaum zu erreichen. Sowohl im Bereich der KI- als auch der Datenschutzaufsicht hätten Unternehmen, Behörden und Bürger:innen es bei einer Bündelung der Zuständigkeiten im Regelfall nur mit einer Aufsichtsbehörde zu tun. Zudem verfügen die Datenschutzaufsichtsbehörden nicht nur über einschlägige Fachkunde und die von der KI-VO geforderte Unabhängigkeit, sondern auch über funktionierende Kooperations- und Kohärenzmechanismen.

Ohnehin bleibt die Datenschutzaufsicht – jedenfalls bei KI-Systemen, die personenbezogene Daten verarbeiten, wie dies in der Praxis regelmäßig auftreten wird – vollständig bestehen, da die KI-VO die DSGVO in ihrem Anwendungsbereich nicht ersetzt. Auch die KI-VO erkennt die Expertise der Datenschutzbehörden an: Für Kernelemente der demokratischen Ordnung sind sie bereits zuständige Marktüberwachungsbehörden (Strafverfolgung, Wahlen, Grenzkontrolle und Justizverwaltung, Art. 74 Abs. 8 i. V. m. Anhang III Nr. 1, 6, 7, 8 KI-VO). Als für den Grundrechtsschutz zuständige Behörde erhält die Datenschutzaufsicht im Rahmen ihrer bestehenden Zuständigkeiten zudem zusätzliche Befugnisse für KI-Systeme, die personenbezogene Daten verarbeiten (Art. 77, EG 157 KI-VO). Daher liegt es nahe, den Datenschutzaufsichtsbehörden auch darüber hinaus nach innerstaatlichem Recht Zuständigkeiten zur Durchsetzung der KI-VO zuzuweisen.

Strukturell handelt es sich bei der KI-VO im Wesentlichen um ein Regelwerk der Produktregulierung im Ordnungsrahmen des „New Legislative Frameworks". Künstliche Intelligenz kann dabei nur auf Basis digitaler Rechte und namentlich eines hohen Datenschutzniveaus prosperieren. Als Produktregulierungsverordnung wird die Zuständigkeit für die Marktüberwachung nach der KI-VO Bund und Ländern zugewiesen werden müssen: Während Landesbehörden im Grundsatz die Aufsicht führen, wird eine Bundesbehörde für die einheitliche Regelung gesamtstaatlicher Sachverhalte zuständig sein (Art. 83, 72 Abs. 2 GG). Dies entspricht auch der Struktur der Behörden im Produktsicherheitsrecht, welche die Marktüberwachungs-Verordnung umsetzen (§ 4 MÜG, § 25 ProdSG).

Nationale Regelung der Zuständigkeiten für die KI-VO
Die Benennung der jeweiligen allgemeinen Marktüberwachungsbehörden in den Mitgliedstaaten ist in der KI-VO nicht dediziert geregelt. Es finden sich nur vereinzelt Vorgaben, die bei der nationalen Bestimmung zu berücksichtigen sind. Für Deutschland muss – wie in anderen Mitgliedstaaten auch – in einem nationalen Umsetzungsgesetz festgelegt werden, welcher oder welchen unabhängigen nationalen Behörden die jeweiligen Zuständigkeiten zugewiesen werden (Art. 70 Abs. 1 KI-VO). Dabei muss gleichzeitig auch eine hinreichende Bereitstellung aufgabengerechter zusätzlicher Ressourcen mitgedacht werden.

Die DSK empfiehlt, die allgemeinen Marktüberwachungsbehörden für die Zwecke der KI-VO in Deutschland wie folgt zu benennen:

- Marktüberwachungsbehörden: BfDI und Landesdatenschutzbehörden

  Hinweis: Wird ein KI-System bundesweit als Produkt angeboten oder aus dem internen Gebrauch heraus zum externen Vertrieb auf den Markt gebracht, liegt die Zuständigkeit hierfür beim Bund. Insbesondere die Nutzung oder die Entwicklung von KI-Systemen für den internen Gebrauch durch Unternehmen und Behörden wird von den Landesdatenschutzbehörden bzw. der Bundesdatenschutzbehörde in ihrer jeweiligen Zuständigkeit überwacht.

- Europäischer Ausschuss für KI: BfDI

  Hinweis: Der Vertreter der Mitgliedstaaten im europäischen Ausschuss für KI wird automatisch der zentrale Ansprechpartner gegenüber dem Ausschuss, der Öffentlichkeit und den anderen Akteuren der KI-VO auf nationaler und europäischer Ebene.

- Unberührt bleiben sektorale Zuständigkeiten (z. B. Kraftfahrzeuge, Finanzsektor, KRITIS), soweit sie bereits in dem Verordnungstext vorgesehen sind oder vom Bundesgesetzgeber aufgrund der Sachnähe aufgegriffen werden.

Anhang zum Informationsfreiheitsbericht

Veröffentlichungen der Konferenz der Informationsfreiheitsbeauftragten (IFK) 2023 und 2024

27.11.2024 – Ein modernes Transparenzgesetz für Niedersachsen jetzt!

Auch mehr als 25 Jahre nachdem das erste Informationsfreiheitsgesetz in Kraft trat, ist es in Deutschland noch immer nicht flächendeckend möglich, Ansprüche aus einem Informationsfreiheits- oder Transparenzgesetz geltend zu machen.

Niedersachsen, das neben Bayern über kein Informationsfreiheitsgesetz verfügt, hat sich auf den Weg gemacht, diese Lücke zu schließen. So heißt es im Koalitionsvertrag für die 19. Wahlperiode des Niedersächsischen Landtages:

Für eine freie und transparente Gesellschaft werden wir in Niedersachsen ein modernes und umfassendes Informationsfreiheits- und Transparenzgesetz schaffen. Staatliche Stellen werden dabei verpflichtet, alle relevanten Informationen digital in einem Transparenzregister zu veröffentlichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) begrüßt diesen längst überfälligen Schritt. Aus Sicht der IFK charakterisieren insbesondere folgende Kernelemente ein modernes Transparenzgesetz:

- ein verpflichtendes Transparenzregister oder Transparenzportal,
- eine Zusammenfassung der Regelungen des Umweltinformationsrechtes und des Informationsfreiheitsrechtes in einem Gesetz,
- eine Einbeziehung der kommunalen Ebene in den Transparenzanspruch,
- die Benennung behördlicher Transparenzbeauftragter
- eine Veröffentlichung von individuell auf Antrag zugänglich gemachten Informationen im Transparenzregister, sofern hieran ein öffentliches Interesse besteht,
- eine Reduzierung von Bereichsausnahmen und Ausschlusstatbeständen auf ein absolut notwendiges Minimum.

Die IFK fordert den niedersächsischen Landesgesetzgeber auf, das Vorhaben aus dem Koalitionsvertrag für ein modernes Transparenzgesetz zeitnah in dieser Legislaturperiode umzusetzen.

05.06.2024 – Pflicht zur Informationsfreiheit und Transparenz auch für Kommunen in Hessen und Sachsen!

In den meisten Ländern ist es selbstverständlich, dass auch die Kommunen den Regelungen der Informationsfreiheit unterliegen. Doch die Gesetze in Hessen und Sachsen überlassen es ihren Kommunen, ob sie transparent sein wollen – freiwillig sind es bisher nur wenige.

Diese Ausnahme vom Anwendungsbereich im Sächsischen Transparenzgesetz und Hessischen Datenschutz- und Informationsfreiheitsgesetz ist nicht überzeugend. Sie schneidet die Menschen von genau den Informationen ab, die sie am meisten interessieren, nämlich von Informationen aus ihrem Wohnumfeld. Dazu gehören Dokumente zur Einrichtung von Kindertagesstätten, Unterlagen zur Förderung der Vereinslandschaft und Verträge des öffentlichen Personennahverkehrs.

Im Gegensatz zu Hessen und Sachsen gelten die Transparenz- bzw. Informationsfreiheitsgesetze in allen anderen Ländern selbstverständlich auch für Kommunen. Damit können die Kommunen in den meisten Ländern nicht selbst entscheiden, ob sie Informationen erteilen wollen, sie sind vielmehr hierzu nach Maßgabe des jeweiligen Landesrechts verpflichtet. Und dies zu Recht: Die bisherigen Evaluierungen der Ländergesetze sind zu dem Ergebnis gekommen, dass Befürchtungen zur Überlastung der Kommunen unbegründet waren und sich diese Regelungen in der Praxis bewährt haben. Die Bürgerinnen und Bürger haben von ihrem Recht auf Informationszugang verantwortungsvoll Gebrauch gemacht.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Landesgesetzgeber in Sachsen und Hessen daher auf, auch ihren Bürgerinnen und Bürgern verbindliche Informationszugangsansprüche gegenüber den Kommunen zu gewähren und diese nicht der Entscheidung der einzelnen Kommunen zu überlassen. Es gibt keinen Grund, den Menschen in Sachsen und Hessen weniger Informationen zur Verfügung zu stellen als denen in anderen Ländern.

05.06.2024 – Gleicher Auftrag – gleicher Informationsanspruch gegenüber öffentlich-rechtlichen Rundfunkanstalten!

Der Rat für die zukünftige Entwicklung des öffentlich-rechtlichen Rundfunks (Zukunftsrat) legte am 18. Januar 2024 einen Bericht vor, der weitreichende Vorschläge für eine Reform von ARD, ZDF und Deutschlandradio beinhaltet. Nicht nachvollziehbar ist, dass der Zukunftsrat sich dabei nicht mit Informationszugang und Transparenz für Bürgerinnen und Bürger auseinandergesetzt hat. Zur Modernisierung gehört auch ein bundesweit einheitlicher Anspruch auf Zugang zu den Informationen der öffentlich-rechtlichen Rundfunkanstalten. Ausgenommen ist nur die grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit. Auch angesichts der bei einzelnen Rundfunkanstalten bekannt gewordenen Krisen und Skandale, wie zum Beispiel umstrittene Zahlungen an einzelne Führungskräfte, ist größtmögliche Transparenz in diesem Bereich unbedingt notwendig. Die Bürgerinnen und Bürger müssen sich einen unmittelbaren Eindruck über die Tätigkeiten der von ihnen finanzierten Anstalten verschaffen können.

Wird derzeit ein Antrag auf Informationszugang gestellt, ergibt sich bezogen auf die unterschiedliche Rechtslage in den einzelnen Ländern ein zersplittertes Bild mit einem sehr unterschiedlichen Anspruchsniveau. Obwohl alle öffentlich-rechtlichen Rundfunkanstalten im Kern den gleichen Auftrag haben, hängt das Ob und Wie des Informationsanspruchs vom Sitz der jeweiligen Rundfunkanstalt ab. In Ländern mit Mehrländeranstalten scheitert ein wirksamer Informationszugangsanspruch häufig sogar ganz an dem Erfordernis, dass dieser staatsvertraglich geregelt sein muss und eine entsprechende Regelung fehlt.

Wo erforderlich, müssen daher entsprechende gesetzliche Regelungen getroffen werden. Die Transparenzansprüche sollten dabei möglichst weit reichen und auch für Themen wie beispielsweise Produktionskosten, Vermögensgeschäfte oder Spitzenvergütungen gelten. Der Informationszugang muss von unabhängigen Stellen kontrolliert werden, das heißt, dort wo vorhanden durch die Informationsfreiheits- und Transparenzbeauftragten des Bundes und der Länder.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher bundesweit einheitlich hohe Standards für den Anspruch auf Informationszugang gegenüber öffentlich-rechtlichen Rundfunkanstalten. Der öffentlich-rechtliche Rundfunk ist Medium und Faktor öffentlicher Meinungsbildung. Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber daher auf, auch in diesem Bereich für Transparenz zu sorgen und dadurch die Unabhängigkeit des öffentlich-rechtlichen Rundfunks zu stärken.

04.06.2024 – Gut informiert im Superwahljahr 2024!

2024 ist ein Superwahljahr: Europawahl, drei Landtagswahlen und verschiedene Kommunalwahlen stehen an. Wahlen stellen das zentrale Mittel dar, mit dem Wählerinnen und Wähler ihrer vom Grundgesetz zugedachten Rolle nachkommen können: „Alle Staatsgewalt geht vom Volke aus.“ Mit dem allgemeinen Wahlrecht erfüllt sich der Anspruch auf demokratische Teilhabe.

Wählerinnen und Wähler sind auf Informationen aus zuverlässigen Quellen angewiesen. Allgemeine Informationen zur Wahl sind etwa bei den Bundes- bzw. Landeswahlleitungen und den Zentralen für politische Bildung erhältlich. Letztere stellen insbesondere Informationen über die Wahlprogramme der politischen Parteien zur Verfügung. Die Inhalte der Wahlprogramme werden z. B. in Wahl-O-Maten gebündelt und bieten für manche eine hilfreiche Grundlage für die Wahlentscheidung. Die Wahlprogramme umfassen allerdings nur die Vorhaben und Absichtserklärungen der Parteien.

Einen unmittelbaren Einblick in das Regierungs- und Verwaltungshandeln in der zurückliegenden Wahlperiode können amtliche Informationen geben, die auf Grundlage verschiedener Gesetze im Bund und den meisten Ländern mittels Informationszugangsantrags beansprucht werden können oder bereits proaktiv veröffentlicht werden. Zur Verfügung stehen hierfür vor allem Transparenz-, Informationsfreiheits-, und Umweltinformationsgesetze. Auf diese Weise besteht die Möglichkeit zum Zugang zu Informationen aus erster Hand, die einen ungefilterten Eindruck über die tatsächliche Arbeit von Regierung und Verwaltung geben. Sie können eine wichtige Grundlage für eine fundierte Meinungsbildung beziehungsweise öffentliche Diskussion sein.

Da gerade im Wahlkampf auch Desinformation, also gezielte Falschinformation, ein Mittel sein kann, um die öffentliche Meinung und auch Wahlentscheidungen zu beeinflussen, sollten sich die Wählerinnen und Wähler ihrer Informationsrechte bewusst sein. Originalinformationen sind so wichtig wie nie. Diese sind eine valide und seriöse Grundlage, um später an der Wahlurne gut informiert und sachorientiert zu entscheiden.

Daher weist die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Wählerinnen und Wähler darauf hin, dass die Gesetze über Transparenz und Informationsfreiheit besonders vor Wahlen ein geeignetes Mittel sein können, um sich fundiert zu informieren.

14.06.2023 – Die Demokratie braucht starke Medien – Bundespressegesetz jetzt einführen!

Der Bund verfügt im Gegensatz zu den Ländern nicht über ein Pressegesetz. Bis zum Jahr 2013 hat sich die Presse für ihren Auskunftsanspruch auch gegenüber Bundesbehörden auf die Pressegesetze der Länder berufen. 2013 hat das Bundesverwaltungsgericht jedoch entschieden, dass dies unzulässig sei. Vielmehr ergebe sich der presserechtliche Auskunftsanspruch gegenüber Bundesbehörden unmittelbar aus dem Recht auf Pressefreiheit aus dem Grundgesetz. Es sei Sache des Bundesgesetzgebers, einen Informationszugang zu regeln (Bundesverwaltungsgericht, Urteil vom 20. Februar 2013, Az.: 6 A 2.12), der jedenfalls nicht hinter den landespresserechtlichen Ansprüchen zurückbleiben darf (Bundesverwaltungsgericht, Urteil vom 8. Juli 2021, Az.: 6 A 10.20).

Auch zehn Jahre nach der Entscheidung fehlt eine konkrete Ausgestaltung und damit die Rechtssicherheit, ob und wie Bundesbehörden der Presse Auskunft zu gewähren haben. Der alleinige Rückgriff auf das Informationsfreiheitsgesetz des Bundes wird der von Verfassungs wegen gebotenen besonderen Stellung der Medien nicht gerecht. Die Regierungsparteien haben sich in ihrem Koalitionsvertrag darauf verständigt, diese Lücke zu schließen. Ein konkreter Gesetzentwurf für ein Bundespressegesetz steht aber nach wie vor aus.

Eine starke Presse ist für eine lebendige Demokratie existenziell. Dazu ist sie auf einen raschen und umfassenden Informationszugang angewiesen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert den Bundesgesetzgeber auf, zeitnah ein effizientes Bundespressegesetz zu schaffen, das der herausragenden Rolle der Presse und den Erfordernissen einer modernen Medienlandschaft Rechnung trägt.

07.11.2023 – Künstliche Intelligenz (KI) verantwortungsvoll für die Informationsbereitstellung nutzen!

Künstliche Intelligenz (KI) kann bei der Umsetzung der Informationsfreiheit helfen. Die schnelle und fristwahrende Umsetzung der gesetzlich vorgeschriebenen Transparenz von Behördenhandeln scheitert immer wieder am Aufwand bei der Sichtung der vorhandenen Informationen und deren Bewertung durch die informationspflichtige Stelle.

KI ist auf dem digitalen Vormarsch und wird vermehrt im Alltag eingesetzt. Durch ihren Einsatz können organisatorische Abläufe optimiert und Arbeitsschritte automatisiert werden. Auch für die Informationsfreiheit kann das Potenzial von KI genutzt werden, um die Bereitstellung von amtlichen Informationen zu vereinfachen und damit zu fördern.

Es werden bereits Prototypen von KI-Tools genutzt, die bspw. durch Zusammenfassungsfunktionen oder Fließtextgenerierung die Arbeit der Verwaltungsmitarbeitenden unterstützen. Im Justizbereich gibt es u. a. auch Projekte, bei denen zum Beispiel gerichtliche Entscheidungen mithilfe von KI-basierten Schwärzungstools veröffentlicht werden können.

Was beim Einsatz von KI aber immer beachtet werden muss: KI ist ein „Werkzeug", das für den optimalen Einsatz durch den Menschen korrekt angelernt und überwacht werden muss, um amtliche Informationen zu sondieren und Fehler bei deren Einschätzung zu vermeiden. Beim Einsatz von KI durch öffentliche Stellen muss deshalb gewährleistet sein, dass die eingesetzten Verfahren durch ausreichende Transparenz und durch technisch-organisatorische Gestaltung überprüfbar und beherrschbar sind. Gesetzliche Bestimmungen und ethische Grundsätze sind dabei zu berücksichtigen. Dazu gehören auch der Persönlichkeitsrechtsschutz und die datenschutzrechtlichen Vorgaben.

So können perspektivisch in wenigen Schritten beantragte Informationen bereitgestellt werden. Ebenso kann auch die proaktive Veröffentlichung im Rahmen der Transparenzportale erleichtert werden. Die abschließende Entscheidung muss jedoch zwingend durch den Menschen erfolgen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) sieht die KI unter Beachtung der o. g. Grundsätze im Informationsfreiheitsbereich als ein effektives Instrument zur schnellen Informationsbereitstellung an.

07.11.2023 – 25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz!

Nach 25 Jahren Århus-Konvention ist die so wichtige proaktive Veröffentlichung von Umweltinformationen in Deutschland immer noch abhängig vom Transparenzwillen der Behörden. Das muss sich ändern.

Mit der Århus-Konvention wurden 1998 erstmals internationale Mindeststandards für den Zugang zu Umweltinformationen völkerrechtlich verankert. Das Übereinkommen fußt auf der Erkenntnis, „daß jeder Mensch (...) die Pflicht hat, die Umwelt zum Wohle gegenwärtiger und künftiger Generationen zu schützen und zu verbessern" und „zur Wahrnehmung dieser Pflicht Zugang zu Informationen, ein Recht auf Beteiligung an Entscheidungsverfahren und Zugang zu Gerichten in Umweltangelegenheiten haben" muss.

Die Bestimmungen der Konvention fanden durch die EU-Umweltrichtlinie aus dem Jahr 2003 Eingang ins Gemeinschaftsrecht und im Folgenden

ins nationale Recht. So sehen die Umweltinformationsgesetze in Deutschland vor, dass Behörden Umweltinformationen proaktiv und nicht nur auf Antrag Einzelner veröffentlichen müssen. Allerdings stellt diese Pflicht zur „Unterrichtung der Öffentlichkeit" in den allermeisten Ländern und auf Bundesebene keinen selbständigen, einklagbaren Anspruch für jedermann dar.

Bei Verstößen gegen die Pflicht fehlt somit die Möglichkeit zur Durchsetzung: Die Nichtbeachtung ist nach aktueller Gesetzeslage nicht gerichtlich überprüfbar und die bloße Veröffentlichungspflicht droht zu verpuffen. Nur in den Transparenzgesetzen von Hamburg, Bremen und Rheinland-Pfalz besteht bislang – in gewissem Maße – ein subjektives Recht auf Veröffentlichung.

Um die Bürgerinnen und Bürger bei der Wahrnehmung ihres Rechts auf Zugang zu Umweltinformationen – ganz im Geiste der Århus-Konvention – zu stärken, ist eine Novellierung des Umweltinformationszugangsrechts nötig. Die IFK fordert die bisher untätigen Gesetzgeber dazu auf, die Verpflichtung zur Unterrichtung der Öffentlichkeit zu modernisieren und als selbständigen Anspruch zu formulieren.

07.11.2023 – Moderne Transparenzgesetze bundesweit – für eine lebendige Demokratie!

Die Informationsfreiheitsgesetze sind ein wichtiges Instrument, um die Akzeptanz der Demokratie zu befördern. Sie ermöglichen durch einen allgemeinen und voraussetzungslosen Zugang zu Informationen Beteiligung und Kontrolle.

Betrachtet man die existierenden Regelungen über den Zugang zu amtlichen Informationen, so gibt es in Deutschland derzeit eine „Drei-Klassen-Gesellschaft":

In einigen Bundesländern gibt es Transparenzgesetze mit proaktiven Veröffentlichungspflichten auf staatlichen Transparenzplattformen. In einigen Ländern und im Bund gibt es Informationsfreiheitsgesetze, die den Informationszugang nur auf Antrag gewähren. In Bayern und Niedersachsen gibt es nach wie vor kein voraussetzungsloses Recht auf Zugang zu amtlichen Informationen.

Moderne Transparenzgesetze zeichnen sich im Kern dadurch aus, dass sie die proaktive Informationsbereitstellung in Transparenzportalen durch öffentliche Stellen der Bundes-, Landes sowie der kommunalen Ebene gewährleisten.

Darüber hinaus sollten bei der Ausgestaltung moderner Transparenzgesetze weitere wichtige Gesichtspunkte einbezogen werden:

- die Zusammenlegung von IFG und UIG,
- den Verzicht auf Bereichsausnahmen,
- die Möglichkeit einer niedrigschwelligen Antragstellung,
- die Pflicht zur Abwägung mit dem öffentlichen Interesse an der Bekanntgabe von Informationen bei bestehenden Geheimhaltungsinteressen und
- Reduzierung und Harmonisierung der Ausschlussgründe

Die IFK fordert die Bundes- und Landesgesetzgeber dazu auf, mit modernen Transparenzgesetzen das Recht auf Informationszugang deutschlandweit auf ein einheitlich hohes Niveau zu bringen und die Informationsfreiheits- und Transparenzbeauftragten des Bundes und der Länder mit den erforderlichen Kompetenzen auszustatten.

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DS-GVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss (englisch: European Data Protection Board: EDPB)
IFG NRW	Informationsfreiheitsgesetz Nordrhein-Westfalen
JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016
KI-VO	Verordnung (EU) 2024/1689 - Verordnung über künstliche Intelligenz
TKG	Telekommunikationsgesetz

Bildnachweise

Abbildung 1 | Seite 7 – LDI NRW;
Abbildung 2 | Seite 13 – Bildagentur PantherMedia / artjazz;
Abbildung 3 | Seite 17 – Datenschutzkonferenz;
Abbildung 4 | Seite 21 – Bildagentur PantherMedia / Raul Ruiz;
Abbildung 5 | Seite 23 – Bildagentur PantherMedia / AndreyPopov;
Abbildung 6 | Seite 36 – Bildagentur PantherMedia / Natalia Danko;
Abbildung 7 | Seite 41 – Bildagentur PantherMedia / Yuri Arcurs;
Abbildung 8 | Seite 47 – Bildagentur PantherMedia / Yuri Arcurs;
Abbildung 9 | Seite 55 – Bildagentur PantherMedia / Harry Huber;
Abbildung 10 | Seite 64 – Bildagentur PantherMedia / AndreyPopov;
Abbildung 11 | Seite 66 – Bildagentur PantherMedia / heiko119,
Abbildung 12 | Seite 71 – Bildagentur PantherMedia / Olaf Schlüter;
Abbildung 13 | Seite 75 – Bildagentur PantherMedia / dpcrestock (Srdjan Draskovic);
Abbildung 14 | Seite 79 – Bildagentur PantherMedia / vilevi (YAYMicro);
Abbildung 15 | Seite 82 – Bildagentur PantherMedia / towfiq007 (YAYMicro);
Abbildung 16 | Seite 89 – Bildagentur PantherMedia / Funtap;
Abbildung 17 | Seite 95 – Bildagentur PantherMedia / Andriy Popov;
Abbildung 18 | Seite 100 – Bildagentur PantherMedia / Funtap;
Abbildung 19 | Seite 107 – Bildagentur PantherMedia / Frank Gärtner;
Abbildung 20 | Seite 113 – Bildagentur PantherMedia / Bernd Leitner;
Abbildung 21 | Seite 119 – Bildagentur PantherMedia / smuki;
Abbildung 22 | Seite 123 – Bildagentur PantherMedia / Andriy Popov;
Abbildung 23 | Seite 127 – Bildagentur PantherMedia / Andriy Popov;
Abbildung 24 | Seite 130 – Bildagentur PantherMedia / Deyan Georgiev;
Abbildung 25 | Seite 135 – Bildagentur PantherMedia / Denniro,
Abbildung 26 | Seite 139 – Bildagentur PantherMedia / Birgit Strehl,
Abbildung 27 | Seite 141 – Bildagentur PantherMedia / dotshock (YAYMicro);
Abbildung 28 | Seite 147 – Bildagentur PantherMedia / Andriy Popov,
Abbildung 29 | Seite 153 – Bildagentur PantherMedia / maxkabakov (YAYMicro);
Abbildung 30 | Seite 157 – Bildagentur PantherMedia / Andriy Popov;
Abbildung 31 | Seite 161 – Bildagentur PantherMedia / Anke Leifeld;
Abbildung 32 | Seite 164 – Bildagentur PantherMedia / Antonio Guillen Fernández;
Abbildung 33 | Seite 166 – Bildagentur PantherMedia / Jürgen Wöhrle;
Abbildung 34 | Seite 173 – Bildagentur PantherMedia / Antje Lindert-Rottke;

Impressum

Herausgeberin:
Bettina Gayk
Landesbeauftragte für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Kavalleriestraße 2–4
40213 Düsseldorf

Tel.: 0211 / 384 24 - 0
Fax: 0211 / 384 24 - 999
E-Mail: poststelle@ldi.nrw.de

Dieser Bericht kann unter www.ldi.nrw.de abgerufen werden.
Zitiervorschlag: 30. Bericht LDI NRW
ISSN: 0179–2431
Düsseldorf 2024

Gedruckt auf chlorfreiem Recyclingpapier

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
www.ldi.nrw.de